# TALTEORI

AF

JULIUS PETERSEN

UDGIVET MED BIDRAG AF UNIVERSITETETS
FRITRYKSKONTO

KØBENHAVN
TRYKT HOS J. H. SCHULTZ A/S
1909

QA241
P4
Mathematics

# INDLEDNING

De ældste Oplysninger, man har, om Folkeslagenes Kendskab til Tal og Regnekunst, skrive sig fra c. 3500 Aar før vor Tidsregning. Man ved, at Kineserne den Gang benyttede Snore med Knuder og Kugler til at repræsentere de ni første Tal. I en Tabel Lo-chou*) ere de ordnede i ni smaa Kvadrater, som danne det, vi nu kalde et Tryllekvadrat; skrevne med vore Cifre ser Tabellen saaledes ud:

| | | |
|---|---|---|
| 4 | 9 | 2 |
| 3 | 5 | 7 |
| 8 | 1 | 6 |

Fra Ægypterne have vi c. 1700 Aar f. Chr. Kong *Ahmes* Regnebog, der indeholder Opløsning af alle Brøker med Tælleren 2 og Nævnere op til 99 i Summer af Stambrøker, det vil sige Brøker med Tælleren 1 og simplere Nævnere. Lige saa gamle ere babyloniske Indskrifter, der udtrykke Kvadrattallene til $60^2$ og Kubiktallene til $32^3$ i et Talsystem med Grundtal 60.

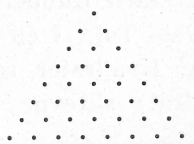
*Pythagoras* (569—470 f. Chr.) opholdt sig i lang Tid i Ægypten og har sandsynligvis der hentet endel af sin

*) *Lucas:* La nature, 1ste Marts 1890.



346468

matematiske Viden; han skal ogsaa have været nogen Tid som Fange i Babylon. Ved sin Hjemkomst dannede han i Syditalien den pythagoræiske Skole. Da de græske Skoler vare meget hemmelighedsfulde, kan man ikke stole paa, at de Opdagelser, der tilskrives Stifteren, virkelig hidrøre fra ham. Man ved, at Skolen, hvad Talteorien angaar, beskæftigede sig med visse særegne Klasser af Tal og Talforbindelser. Trekantstallene ere Summer af de første hele Tal, altsaa Tal af Formen $\frac{1}{2}n(n+1)$. Navnet hidrører fra, at Tallene angive Antallet af Prikker i en Trekant, der er dannet, som Figuren viser:



Paa lignende Maade kommer man til Firkantstal og andre Polygontal. De udtrykke alle Summerne af simple Differensrækker; navnlig kan mærkes, at Firkantstallene bestemme Kvadrattallene som Summer af de første ulige Tal. Idet man herved faar

$$(n+1)^2 - n^2 = 2n + 1$$

og bestemmer $n$ saaledes, at $2n+1$ er et Kvadrattal, faas Løsninger i hele Tal af den ubestemte Ligning

$$x^2 + y^2 = z^2$$

Lægges Trekanter som den ovenfor, og hvis Sider indeholde $n, n-1 \ldots 2,$[1] Prikker ovenpaa hinanden (Kuglestabler) kommer man til Pyramidaltallene; de ere Summer af de første Trekantstal (Polygontal), og disse danne en Differensrække af anden Orden.



Fuldkomne Tal ere Tal, der ere lig Summen af deres aliquote Dele (Divisorer, hvor Tallet selv ikke medregnes) og venskabelige Tal to saadanne, af hvilke ethvert er lig Summen af det andets aliquote Dele.

Talteorien synes ikke at være udviklet videre i de første Aarhundreder efter Pythagoræerne; noget bestemt om dens Stilling lærer vi først af *Euclid* (c. 315—255 f. Chr.) i 7de, 8de og 9de Bog af hans Elementer. Han begynder med at vise Metoden til Bestemmelse af to Tals største fælles Maal og slutter deraf, at et Tal, der gaar op i to andre, ogsaa gaar op i deres største fælles Maal; han behøver nu kun den Sætning, at naar $a$ og $b$ ere indbyrdes primiske, vil $k$ være største fælles Maal for $ka$ og $kb$ for straks at komme til Aritmetikkens Fundamentalsætning, at et Tal kun kan opløses i eet System af Primfaktorer, men den nævnte Sætning findes ikke, medens han gennem en Udvikling af en Proportionslære for rationale Tal kommer til et ikke uangribeligt Bevis for den Sætning, at naar $a$ og $b$ ikke ere delelige med Primtallet $p$, er $ab$ det heller ikke, en Sætning, af hvilken Fundamentalsætningen let udledes.

Euclid har forøvrigt i de nævnte Bøger en Mængde Sætninger om Primtal og sammensatte Tal; han ender 9de Bog med den Sætning, at $(1+2+2^2+\ldots 2^n)\,2^n$ er et fuldkomment Tal, naar den første Faktor er et Primtal. Vi vise senere (se 7), at der ikke gives andre lige fuldkomne Tal end de saaledes bestemte. I 10de Bog viser han, at Primtalrækken er uendelig.

Efter Euclid gik der mange Aarhundreder, i hvilke Erhvervelserne paa Talteoriens Omraade vare ubetydelige. Archimedes († 212 f. Chr.) fandt Summen af de $n$ første Kvadrattal, og Summen af de $n$ første Kubiktal

synes ogsaa at have været kendt. Forøvrigt beskæftigede man sig med at søge Betingelser for, at kvadratiske Ligninger havde rationale Rødder, med Figurtallene o. s. v., men i det hele taget var Matematikernes Interesse henvendt paa Geometrien, og selve de faa og spredte aritmetiske Undersøgelser fik geometrisk Form.

Først i Midten af det fjerde Aarhundrede af vor Tidsregning finde vi i *Diophants* Aritmetik Fremskridt af Betydning. Værket blev kommenteret af den lærde Hypathia, Theons Datter, der underviste i Alexandria omkring Aar 400. Af Værkets 13 Bøger ere de 7 tabte. Vi have nu kun de 6 første med Noter af Munken *Maximus Planudes*, der levede henimod Midten af det 13de Aarhundrede. En Oversættelse paa Latin med Kommentarer af Xylander i 1575 er fuld af Fejl. Den bedste Udgave (Græsk og Latin) med Kommentarer og Tilføjelser skyldes *Bachet* og udkom i Paris 1621. Fermat, som vi senere skulle omtale udførligere, havde forsynet sit Eksemplar med en Mængde Randnoter, og hans Søn offentliggjorde i 1670*) en ny Udgave, forøget med Faderens Noter og Opdagelser. I 1890 er der udkommet en tysk Udgave med Noter af Wertheim. En fransk Udgave, „œuvres de Fermat“ er udgivet af P. Tannery og Henry. Diophant beskæftigede sig særlig med ubestemte Ligninger af anden Grad, for hvilke han søger rationale Løsninger. Han giver ingen almindelige Teorier, men stiller en Mængde specielle Opgaver, der fører til saadanne Ligninger, og som han behandler med stor Behændighed. Han forlader den ældre geometriske Form og indfører en særlig Betegnelse for den ubekendte,

*) Se ogsaa Fermatii opera math. Tolosae 1679.



medens han for de bekendte Størrelser sætter vilkaarlige Tal.

I Middelalderen delte Talteorien Videnskabens almindelige Skæbne blandt de europæiske Nationer; det var hos Inderne, og særlig hos Araberne, at den fordrevne Matematik fik et Hjem, fra hvilket det ved Renaissancen atter kunde vende tilbage til Europa. Det var fra Inderne, der vare store Regnemestre, at vi gennem Araberne fik vor nuværende Maade at skrive Tallene paa. Mange af de bedste græske Forfattere bleve oversatte paa Arabisk og derved bevarede fra Undergang. Af Arabernes selvstændige Arbejder paa Talteoriens Omraade skulle vi nævne, at man fra det 9de Aarhundrede har følgende Bestemmelse af venskabelige Tal:

Naar

$$p = 3.2^n - 1,\ q = 3.2^{n-1} - 1 \text{ og } r = 9.2^{2n-1} - 1$$

alle ere Primtal, saa ere

$$2^n pq \text{ og } 2^n r$$

venskabelige Tal. Fra omtrent Aaret 1000 har man Sætningen, at Summen af to Kubiktal ikke atter kan være et Kubiktal. Archimedes havde, som tidligere anført, fundet Summen af de $n$ første Kvadrattal, Araberne finde Summen af de $n$ første Kubiktal og af de $n$ første Bikvadrattal. De dannede ikke alene Tryllekvadrater med 9, men ogsaa med 16, 25 og 36 Felter. (Opstillingen af de $n^2$ første Tal i Felterne af et Tryllekvadrat skal være saaledes, at Summerne af Tallene i alle Rækker og Søjler og i Diagonalrækkerne skal være den samme). *Bossut* tilskriver en græsk Munk Mochopulus, der levede i Begyndelsen af det femtende Aarhundrede, Opfindelsen af Tryllekvadrater, men de vare, som vi have set, kendte langt tidligere.

Naar vi nu vende os til den Tid, da man atter begyndte at dyrke Talteorien i Europa, maa vi særlig nævne *Bachet de Miziriac* (1577—1638), som vi tidligere have omtalt som Udgiver af Diophant. Uagtet *Vieta* dengang havde indført ogsaa at betegne bekendte Størrelser ved Bogstaver, følger Bachet Diophant deri, at han kun indfører en Bogstavbetegnelse for den ubekendte. Han maa betragtes som den Europæer, der først giver en almindelig Metode til Løsning af den ubestemte Ligning af første Grad*), en Metode, der falder nær sammen med vor nuværende Løsning ved Kædebrøk. Han lærte at danne Tryllekvadrater med et ulige Antal Felter. Det var især i Værket Problèmes plaisans et delectables, at han anvendte sine Metoder paa mange forskellige Opgaver. Den første Udgave udkom i Lyon 1612; anden Udgave er fra 1624; tredje af *A. Labosne* fra 1874 (Paris).

Tryllekvadrater have forøvrigt ogsaa senere beskæftiget mange Matematikere, saaledes *Fermat* og hans samtidige, *Frénicle*, et af de første Medlemmer af det nylig oprettede Académie française, endvidere *Poignard*, Bryssel 1703, *Lahire*, Mém. de l'Acad., *Sauveur*, Mém. 1710, *Osembrai* 1750 og *Railler de Ourmes* sammesteds 1763.

Som den, der, hvad Talteorien angaar, ragede højt over sine Forgængere og Samtidige maa vi nævne den ogsaa paa andre Punkter udmærkede Matematiker *Fermat* (1601—1665). I hans Randnoter til Diophant og i hans Korrespondance med andre Matematikere, særlig med Frénicle, finde vi en Mængde talteoretiske Sætninger, de fleste uden Bevis. Den vigtigste var den berømte fermatske Sætning, at et Primtal $p$ gaar op i

*) Inderne havde tidligere løst saadanne Ligninger.



$a^{p-1}-1$, naar det ikke gaar op i $a$; denne Sætning bevistes og udvidedes af Euler, der har beskæftiget sig meget med de fermatske Sætninger. Om en af disse, nemlig at $2^n + 1$ var et Primtal, naar $n$ var en Potens af 2, viste Euler, at den var urigtig, idet $2^{32} + 1$ er delelig med 641. Fermat havde forøvrigt indrømmet, at han ikke havde Bevis for Sætningen.

Fermat opstiller den Sætning, at ethvert Tal kan skrives som en Sum af højst 3 Trekantstal, 4 Firkantstal (Kvadrater), 5 Femkantstal o. s. v. Den anden af disse Sætninger havde Bachet forgæves forsøgt at bevise. Fermat beskæftigede sig med fuldkomne Tal og lignende Talformer; han paastaar, at han af Tallet 120, der er halvt saa stort som Summen af dets aliqvote Dele, har udledt et andet, 672, med samme Egenskab, ligesom at han af de to venskabelige Tal 220 og 284 har udledt de to andre, 17296 og 18416. Disse Tal ere dog saadanne, som bestemmes ved den Pg. 5 angivne arabiske Regel.

En Sætning af Bachet udvides af Fermat til følgende: Hvis Ligningen $x^3 + y^3 = a$ har et Sæt rationale Løsninger, har den uendelig mange.

Denne Sætnings Rigtighed indses lettest ved en geometrisk Betragtning. Ligningen kan opfattes som Ligning for en Kurve af tredje Orden med et rationalt Punkt; en Tangent til dette vil skære Kurven i et nyt rationalt Punkt og saaledes videre, ligesom en Linie gennem to rationale Punkter bestemmer et nyt rationalt Punkt. Om man paa denne Maade faar alle Løsninger, er ikke bevist. Hvis det givne rationale Punkt er et Vendepunkt, bestemmer Metoden intet nyt rationalt Punkt. Saaledes vil f. Eks. for $a = 1$ det rationale Punkt (0,1) ikke bestemme ny rationale Løsninger.

Fermat undersøger Tals Deling i en Sum af to ind-

byrdes primiske Kvadrater og viser, at saadanne Tal kun kunne indeholde Primfaktorer af Formen $4n + 1$ og Faktoren 2. Omvendt kan ethvert Primtal af Formen $4n + 1$ skrives som en Sum af to Kvadrater og det kun paa een Maade. Produktet af to Summer af to Kvadrater kan atter skrives som en Sum af to Kvadrater, idet

$$(x^2 + y^2)(a^2 + b^2) = (ax \pm by)^2 + (bx \mp ay)^2$$

en Identitet, som forøvrigt allerede var kendt af Diophant.

En vigtig Opgave, som Fermat forelagde Samtidens Matematikere, er den, at vise, at Ligningen

$$ax^2 + 1 = y^2$$

har uendelig mange Løsninger. Opgaven løstes besværligt af Englænderne *Brouncker* og *Wallis*; Ligningen har paa Grund af en Fejltagelse af Euler faaet Navnet den *Pellske* Ligning. Den var allerede behandlet af Inderne, men, som sædvanligt hos disse, uden Begrundelse; en saadan blev givet af *Lagrange*, der genfandt Indernes Metode.

Af fermatske Sætninger skulle vi endnu blot nævne den, at der ikke eksisterer retvinklede Trekanter, hvis Sider og Areal ere hele Tal, den, at Summen eller Differensen af to Bikvadrattal ikke kan være et Kvadrattal og saa meget mindre et Bikvadrattal og endelig den berømte under Navnet Fermats sidste Sætning bekendte Paastand, at Ligningen

$$x^n + y^n = z^n$$

kun kan løses i hele Tal for $n = 2$. For $n = 3$ var Sætningen, som tidligere omtalt, funden af Araberne.



Den har i høj Grad beskæftiget Matematikerne og er bevist for forskellige Værdier af $n$ navnlig af Kummer, men det er ikke endnu lykkedes at finde et almindeligt Bevis.

Paa Fermats Tid var det Skik, at Matematikerne udfordrede hinanden til at løse Opgaver, de stillede, og Fermats Sætninger fik derved en stor indirekte Betydning.

Foruden *Frénicle*, som vi have omtalt, kunne vi nævne *Descartes, Mersenne, Wallis* o. fl. Det var imidlertid særlig *Euler*, der omkring Midten af det 18de Aarhundrede optog de Fermatske Sætninger og lignende Spørgsmaal til Behandling. I det den Gang nyoprettede Petersborger Akademis Skrifter offentliggjorde han sine Resultater. Vi have allerede blandt disse nævnt, at han fandt Faktoren 641 i Tallet $2^{32} + 1$. Han beviste Fermats Sætning og udvidede den til Divisorer, der ikke ere Primtal*). Han beviste, at et Primtal af Formen $4n + 1$ kan skrives som en Sum af to Kvadrattal, at et Primtal af Formen $6n + 1$ kan bringes paa Formen $x^2 + 3y^2$, og mange analoge Sætninger. *Lagrange* søgte Formen af Divisorerne i mere almindelige kvadratiske, homogene Former*). Han gav desuden i 1771 to Beviser for den Wilsonske Sætning. Denne, der siger, at et Primtal $p$ gaar op i $1 . 2 . 3 \ldots (p-1) + 1$ var i 1770 offentliggjort uden Bevis af *Waring*, der tilskrev en af sine Elever, *John Wilson*, den. Han udvidede den af Euler opstillede Sætning, at Produktet af Tal af Formen $x^2 + y^2 + z^2 + v^2$ atter kan skrives paa samme Form til Faktorer af Formen $x^2 + \alpha y^2 + \beta^2 z + \alpha\beta v^2$.

Medens de talteoretiske Undersøgelser hidtil have

*) Commentat. nov. act. Petrop. VIII.

haft en spredt og tilfældig Karakter, udkom i 1799 og 1801 to Værker, som maa betragtes som de grundlæggende for den videnskabelige Talteori. Det første var *Legendres:* Essai sur la théorie des nombres. Det samler Eulers og Lagranges Undersøgelser af Fermats Sætninger, men føjer dertil mange selvstændige Opdagelser. Blandt disse maa fremfor alt nævnes Reciprocitetsloven for de kvadratiske Rester. I Talteorien er det ofte vanskeligt at sige, hvad der skal kaldes en Løsning af en Opgave; en Løsning ligger ofte lige for Haanden, men er saa besværlig, at den kun kan gennemføres for smaa Tal, og den egentlige Løsning maa da siges at være en saadan, ved hvilken Arbejdet reduceres i høj Grad. Skal man afgøre om $a$ er kvadratisk Rest for et Primtal $p$, kan man dividere $p$ i $a^{\frac{1}{2}(p-1)}$, og man ved da, at $a$ er Kvadratrest, hvis man ved Divisionen faar Resten 1. Men det er tydeligt, at det her krævede Arbejde er uoverkommeligt allerede naar Tallene faa 4 à 5 Cifre. Det er her, at Legendre har givet en Regnemetode (Algorithme), hvorved, særlig efter Metodens Forbedring af Jacobi, Spørgsmaalets Besvarelse selv for Tal med en halv Snes Cifre er let, idet Regningerne omtrent blive de samme som ved Bestemmelse af de to Tals største fælles Maal.

Metoden giver en let Bestemmelse af de lineære Former af Primtal, for hvilke de laveste Tal ere Kvadratrester og derved af saadanne Former, der kunne gaa op i visse simple kvadratiske Former. Saaledes finder man, at $-1$ er Kvadratrest for Primtal af Formen $4n+1$, men ikke for saadanne af Formen $4n+3$, hvoraf umiddelbart følger den Fermatske Sætning, at

*) Mém. de l'acad. de Berlin 1773 og 75.



Summen af to indbyrdes primske Kvadrattal kun har Primfaktorer af Formen $4n+1$.

Legendre gav ikke noget Bevis for sin Sætning, men Gauss gav en hel Række Beviser, i hvilke mange andre, der senere ere fremkomne, have deres Forbilleder.

Legendres Værk er udkommet i flere Udgaver; den sidste med væsentlige Udvidelser i 1830. En tysk Oversættelse af Maser udkom i Leipzig 1886.

Det andet Hovedværk, der udkom i Leipzig 1801, er *Gauss'* Disquisitiones Arithmeticæ*). Det er især dette, der har dannet Grundlaget for den følgende Tids Undersøgelser. Vi ville vente med at omtale disse, til de finde deres Plads i den følgende Udvikling af Hovedpunkterne af Talteorien paa dens nuværende Standpunkt; vi ville derved forudsætte som bekendt saa meget af Elementerne, som i Reglen findes i de bedre Lærebøger til Skolebrug.

*) Tysk Oversættelse af H. Maser Berlin 1889.

# FØRSTE KAPITEL

—

## OM DIVISORER

### Største fælles Maal.

1. Den Række Operationer (den Algorithme), ved hvilken vi bestemme to hele Tals største fælles Maal, støtter sig paa de to Sætninger:

Et Tal, der gaar op i Dividend og Divisor, gaar ogsaa op i Resten.

Et Tal, der gaar op i Divisor og Resten, gaar ogsaa op i Dividenden.

Idet man nu dividerer det mindste af de givne Tal i det største, Resten i den foregaaende Divisor o. s. v., kan man stadig vælge den ufuldstændige Kvotient saaledes, at man faar aftagende Rester, og da disse ere hele Tal, maa man, efter et endeligt Antal af Divisioner, komme til Resten Nul, og den sidst brugte Divisor er da det søgte største fælles Maal. Man har herved benyttet en i Arithmetikken ofte anvendt Metode, nemlig den, at reducere den stillede Opgave til den samme Opgave for mindre Tal.

Man maa vel lægge Mærke til, at det afgørende ved Beviset er, at man efter et endeligt Antal Operationer kommer til Resten Nul; det er ikke nok, at Re-



sterne ere aftagende, thi en Række aftagende positive Størrelser kan godt have en Grænse, der er større end Nul.

2. Efter at Euclid har udviklet Metoden til Bestemmelse af to Tals største fælles Maal, kan han straks opstille den Sætning, at et Tal, der gaar op i to andre, gaar ogsaa op i deres største fælles Maal og naar derpaa ad en længere Vej til et (ikke uangribeligt) Bevis for den Sætning, at et Primtal $p$, der ikke gaar op i $a$ eller $b$, heller ikke gaar op i $ab$. Vi benytte derimod den Sætning:

Naar to Tal multipliceres med $m$, bliver deres største fælles Maal ogsaa multipliceret med $m$, og bevise derved, at

Et Tal, som gaar op i et Produkt af to Tal og er indbyrdes primisk med den ene Faktor, maa gaa op i den anden

og komme derved straks til Fundamentalsætningen:

Et Tal kan kun opløses i eet System af Primfaktorer.

3. Man kan paa forskellig Maade udvide Begrebet „Hele Tal“, og hvis dette sker paa en saadan Maade, at man kan angive en endelig Række af Operationer, der fører til et bestemt største fælles Maal for to vilkaarlige af Tallene, da maa den hele Udvikling for et saadant Talsystem blive analog med den, der gælder for vort sædvanlige System. Saaledes kan man betragte alle Tal af Formen $a + b\sqrt{-1}$, hvor $a$ og $b$ ere sædvanlige hele Tal. Man kan her definere de sædvanlige

Regneoperationer, Primtal, største fælles Maal o. s. v. paa sædvanlig Maade. Opererer man nu, for at bestemme to saadanne Tals største fælles Maal paa sædvanlig Maade, kan man ved Divisionerne bestemme Kvotienterne saaledes, at Resternes Modulers Kvadrater, der ere hele Tal i sædvanlig Forstand, stadig maa blive mindre. Man maa derfor efter et endeligt Antal Operationer faa Resten Nul, og ser derved, at Fundamentalsætningen ogsaa gælder for det ny Talsystem. Dette og et andet, der bestaar af Tallene $a + b\alpha$, hvor $\alpha$ er en af de komplekse Rødder i Liningen $x^3 = 1$, medens $a$ og $b$ ere sædvanlige hele Tal, og for hvilket Fundamentalsætningen ogsaa gælder, vil blive nærmere undersøgt i det følgende.

Som Eksempel paa et Talsystem, hvor Fundamentalsætningen ikke gælder, kunne vi nævne Tallene af Formen $a + b\sqrt{-11}$. Ved alle Forsøg paa at danne en Metode til Bestemmelse af to saadanne Tals største fælles Maal vil det vise sig, at Operationerne ikke føre til nogen Afslutning.

4. Naar man siger, at et Polynomium gaar op i et andet, tænker man i Reglen paa Koefficienternes Art. Her ville vi imidlertid forudsætte, at Dividend og Divisor have hele Koefficienter, og for at Divisionen skal gaa op, kræve vi, at Kvotienten skal have hele Koefficienter. Endvidere ville vi ved, at et helt Tal gaar op i et Polynomium, forstaa, at det gaar op i alle dets Koefficienter. Et helt Tal, der ikke gaar op i et Polynomium, kan naturligvis godt gaa op i den Talværdi, som Polynomiet faar, naar vi for den ubestemte indsætter et helt Tal.

Vi tage nu, naar vi søge største fælles Maal for to



Polynomier, ogsaa Hensyn til Talfaktorer, og det kan vise sig, at det største fælles Maal er et helt Tal. Den sædvanlige Udvikling vedbliver at gælde; særligt bemærke vi, at man, for at undgaa Brøk, multiplicerer Dividenden med en Faktor, som ikke gaar op i Divisor eller af denne bortdividerer en Faktor, som ikke gaar op i Dividenden. Heraf følger da, at den tidligere for hele Tal beviste Sætning ogsaa gælder for Polynomier:

Et Tal, som gaar op i et Produkt af to Polynomier og er indbyrdes primisk med det ene, gaar op i det andet.

Ved Hjælp heraf beviser man nu let følgende Sætning:

Dersom et Polynomium med hele Koefficienter kan opløses i et Produkt af to Faktorer med rationelle Koefficienter, kunne Faktorerne skrives med hele Koefficenter.

Antag nemlig

$$f(x) = \varphi(x) \cdot \psi(x),$$

hvor $f(x)$ har hele Koefficienter, medens de to Faktorer kunne have brudne Koefficienter; vi bortskaffe Brøkerne, idet vi paa begge Sider multiplicere med et passende helt Tal $k$, og faa

$$kf(x) = \varphi_1(x)\, \psi_1(x),$$

hvor de to Faktorer nu have hele Koefficienter. Ifølge den ovenfor beviste Sætning maa en Primfaktor i $k$ gaa op i $\varphi_1(x)$ eller i $\psi_1(x)$, saa at den kan bortdivideres, uden at der paa højre Side indføres brudne Koefficienter. Paa samme Maade bortskaffes de øvrige

Primfaktorer i $k$, og vi have da $f(x)$ udtrykt som et Produkt af to Faktorer med hele Koefficienter.

5. Da vi udviklede Metoden til Bestemmelse af største fælles Maal for to Polynomier i $x$, forudsatte vi $x$ ubestemt. Udviklingen gælder ikke, hvis vi for $x$ indsætte et bestemt, helt Tal; dette ligger i, at en Faktor, med hvilken vi, for at undgaa Brøk, multiplicerer Dividenden, maaske for den specielle Værdi af $x$ gaar op i Divisor. Denne Indvending falder bort, dersom Regningen kan gennemføres, uden at det er nødvendigt at indføre Faktorer i Dividenderne, og vi kunne derfor opstille følgende Sætning:

Dersom største fælles Maal for to Polynomier findes, uden at man i Løbet af Regningen indfører Faktorer i Dividenderne for at undgaa Brøk, da vedbliver Resultatet at gælde, naar man for den ubestemte indsætter et vilkaarligt, helt Tal.

Har man saaledes de to Polynomier $x^m - 1$ og $x^n - 1$, da faa alle Resterne samme Form, saa at der ikke indføres nogen Faktor. Ser man kun paa Eksponenterne, da finder man, at Regningerne føre til Bestemmelse af største fælles Maal for $m$ og $n$. Altsaa:

Største fælles Maal for $x^m - 1$ og $x^n - 1$ er $x^\alpha - 1$, hvor $\alpha$ er største fælles Maal for $m$ og $n$, og dette gælder ogsaa, naar man for $x$ sætter et vilkaarligt, helt Tal.

Saaledes er f. Eks. $7^3 - 1$ største fælles Maal for $7^9 - 1$ og $7^{15} - 1$.



## Et Tals Divisorer.

6. Lad

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots . p_n^{\alpha_n} \tag{1}$$

betegne et Tal opløst i Primfaktorer. Alle Divisorer $d_1 d_2 \dots .$ i $n$, 1 og Tallet selv medregnede, ere da alle Leddene i det udviklede Produkt

$$(1 + p_1 + p_1^2 . + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots . . (1 + p_n + p_n^2 + \dots + p_n^{\alpha_n}) = 1 + d_1 + d_2 \dots + n. \tag{2}$$

Lad nu $m$ og $n$ være vilkaarlige hele Tal og $\psi$ en saadan Funktion, at man, under Forudsætning af, at $m$ og $n$ ere indbyrdes primiske, har

$$\psi(m)\,\psi(n) = \psi(mn). \tag{3}$$

Man vil da, naar man for ethvert Led $l$ i en af Paranteserne sætter $\psi\ (l)$, ved Udførelse af Multiplikationerne faa Summen af $\psi$ Funktionerne af alle Divisorerne. Man kan herved, idet man for $\psi$ vælger forskellige Funktioner, der tilfredsstille Betingelsesligningen, udlede en Række Sætninger om et Tals Divisorer. Sætte vi saaledes $\psi\ (m) = 1$, er Betingelsen tilfredsstillet, og vi faa

Antallet af Divisorer i Tallet $n$ er

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots . . (\alpha_n + 1). \tag{4}$$

Sætte vi $\psi(m) = (-1)^r$, hvor $r$ er Antallet af ens eller forskellige Primfaktorer i $m$, blive Leddene i Parenteserne afvekslende 1 og $-1$, og enhver af Parenteserne faar saaledes Værdien 1 eller 0, eftersom Eksponenten $\alpha$ er lige eller ulige. Produktet bliver saaledes

Nul undtagen i det Tilfælde, hvor alle Eksponenterne $\alpha$ ere lige, altsaa $n$ et Kvadrattal; altsaa:

I ethvert Tal, der ikke er et Kvadrattal, er der lige mange Divisorer med et lige Antal og med et ulige Antal Primfaktorer. For et Kvadrattal bliver det første Antal 1 større end det sidste.

Lade vi $r$ ovenfor betyde Antallet af primiske Divisorer af Formen $4n+3$, bliver i (2) $1+p+p^2+p^\alpha$ lig $\alpha+1$, naar $p$ har Formen $4n+1$; har $p$ derimod Formen $4n+3$, bliver Summen 0 eller 1, eftersom $\alpha$ er ulige eller lige.

Paa højre Side faa vi $\psi(d_k) = -1$, naar $d_k$ er af Formen $4n+3$ (altsaa indeholder et ulige Antal Primfaktorer $4n+3$) og $\psi(d_k) = +1$ naar $d_k$ er af Formen $4n+1$.

Vi faa altsaa for et ulige Tal:

Der er lige mange Divisorer af Formen $4n+1$ og af Formen $4n+3$, undtagen i det Tilfælde, hvor alle Primfaktorer af den sidste Form forekomme med lige Eksponent; i dette Tilfælde bliver der saa mange flere Divisorer af første Slags end af anden Slags, som om alle Primfaktorerne af Formen $4n+3$ manglede.

7. Summere vi Kvotientrækkerne i Parenteserne ovenfor, faa vi for Summen $S$ af Tallets Divisorer:

$$S = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_n^{\alpha_n-1}-1}{p_n-1}. \qquad (5)$$



Som tidligere omtalt forstode Pythagoræerne ved et Tals aliquote Dele dets Divisorer, idet dog Tallet selv ikke regnes med. Skal $n$ være et fuldkomment Tal, bliver Betingelsen derfor, at det dobbelte af Tallet er lig $S$. Er $p_1 = 2$, faa vi da

$$\frac{2^{\alpha_1+1}}{2^{\alpha_1+1}-1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = (1+p_2+p_2^2+\ldots p_2^{\alpha_2}) \ldots$$
$$(1+p_3+\ldots)\ldots(1+p_n+\ldots+p_n^{\alpha_n})$$

eller, idet Brøken kan skrives

$$1+\frac{1}{2^{\alpha_1+1}-1},$$

hvor Nævneren maa gaa op i $p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}$,

$$p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n} + p_2^{\beta_2} p_3^{\beta_3} + p_n^{\beta_n} = (1+p_2+p_2^2+p_2^{\alpha_2})$$
$$(1+p_3+\ldots)\ldots(1+p_n+\ldots+p_n^{\alpha_n}),$$

hvor det andet Led paa venstre Side er mindre end det første; da begge Leddene findes mellem Leddene paa højre Side, kan der ikke findes flere Led, saa at Tallet foruden Primfaktoren 2 kun kan have endnu een Primfaktor, og denne i første Potens. Er denne $p$, bliver Ligningen

$$2^{\alpha+1} p = (2^{\alpha+1}-1)(1+p),$$

hvoraf følger

$$p = 2^{\alpha+1}-1.$$

Vi ere saaledes komne til Euclids Løsning og det paa en saadan Maade, at vi have set, at der ikke gives andre lige fuldkomne Tal end de af Euclid bestemte.

Da $p$ er et Primtal, maa Eksponenten til 2 ogsaa være et Primtal. Man faar saaledes:

$$(2^2—1)\,2 = \mathbf{6};\ (2^3—1)\,2^2 = \mathbf{28};\ (2^5—1)\,2^4 = \mathbf{496};\ (2^7—1)\,2^6$$
$$= \mathbf{8128}\ (2^{13}—1)\,2^{12} = \mathbf{33550336}$$

Endvidere faar man Løsninger for Eksponenterne 17, 19, 31 og 61, men ikke for de mellemliggende Primtal.

8. Man kender intet fuldkomment, ulige Tal; for et saadant maatte man have

$$2p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_n^{\alpha_n} = (1 + p_1 + p^2 + \ldots p_1^{\alpha_1})\,(1 + p_2 + p_2^2 \ldots p_2^{\alpha_2})$$
$$\ldots (1 + p_n + p_n^2 \ldots + p_n^{\alpha_n}),$$

hvor alle $p$ ere ulige Primtal). Alle Parenteserne paa een nær maa bestemme ulige Tal, saa at alle Tallene $\alpha$ paa eet nær maa være lige. Dette ene maa være af Formen $4n + 1$ og det tilsvarende Primtal $p_1$ ligeledes, da Parentesen ellers vilde bestemme et Tal, som var deleligt med en højere Potens af 2 end den første. Parentesen er delelig med $p_1 + 1$, saa at $\frac{1}{2}(p_1 + 1)$ maa være sammensat af en eller flere af de andre Primfaktorer, og $p$ saaledes ikke kan være den mindste af de forekommende Primfaktorer. Hvis man saaledes har $p_1 = 5$ eller $p_1 = 13$, maa henholdsvis 3 eller 7 ogsaa være Faktor.

Man kan bevise, at alle de lige Eksponenter ikke kunne være 2. Alle ulige Primtal undtagen 3 ere nemlig af Formen $6n — 1$ eller $6n + 1$. Er $p$ af Formen $6n + 1$, vil 3 gaa op i $(1 + p + p^2)$; da nu Tallet ifølge vor Forudsætning kun maa indeholde Faktoren 3 to Gange, kan det højst indeholde to Primfaktorer af Formen $6n + 1$; men indeholder det Faktoren 3, maa det



ogsaa indeholde $1 + 3 + 3^2 = 13$, $1 + 13 + 13^2 = 3.61$, $1 + 61 + 61^2 = 3.13.97$, $1 + 97 + 97^2 = 3.3169$.

Alle Tallets Primfaktorer maatte derfor være af Formen $6n — 1$. Lad $p$ være en saadan Primfaktor og $q$ en Primfaktor i $p^2 + p + 1$, altsaa ogsaa i $p^3 — 1$. I Følge Fermats Sætning gaar $q$ op i $p^{q-1}—1$. Heraf følger, at hvis $q$ ikke er Faktor i $p — 1$, maa $q — 1$ være et Multiplum af 3 eller, da $q$ er ulige, et Multiplum af 6, altsaa $q$ af Formen $6n + 1$. Tilbage have vi saaledes kun den Mulighed, at $q$ baade gaar op i $p^2 + p \times 1 = (p—1)(p + 2) + 3$, som kun giver $q = 3$, et Tilfælde, som vi allerede have udelukket.

Vi kunne nok angive andre specielle Tilfælde, som ere umulige, men som kun betyde lidt overfor et almindeligt Umulighedsbevis. Det kan ikke nytte at søge dette blot ved Hjælp af Udtrykkenes Størrelse, thi skrives Betingelsen

$$2 = (1 + \frac{1}{p} + \ldots)(1 + \frac{1}{p_2} + \ldots)\ldots$$

falder en Faktor mellem Grænserne $\frac{p+1}{p}$ og $\frac{p}{p—1}$ (for $\alpha = \infty$), saa at Produktet kan komme saa nær som man vil til enhver positiv Værdi større end 1 (Summen af de reciproke Værdier af Primtallene er uendelig og

$$\pi\ (1 + \frac{1}{p}) > \Sigma \frac{1}{p}\Big)$$

Vi kunne for det foreliggende Tilfælde faa en Grænseværdi, idet vi dog ville forudsætte, at den ulige Eksponent er større end 1. Enhver af Parenteserne er da større end $e^{\frac{1}{p}}$, altsaa

$$\Sigma\ \frac{1}{p} < l.2 = 0.69\ldots;$$

medens efter hvad vi fandt ovenfor,

$$\pi \frac{p}{p-1} > 2.$$

**Primfaktorerne i $n!$**

9. Af Tallene 1, 2, 3 ... $n$ gaar Primtallet $p$ op i

$$p,\ 2p,\ 3p \ldots \left(\frac{n}{p}\right) p,$$

hvor Parentesen betegner det største hele Tal, som findes i Brøken*). $p^2$ gaar op i

$$p^2,\ 2p^2,\ 3p^2 \ldots \left(\frac{n}{p^2}\right) p^2$$

og saaledes videre; det Antal Gange Primfaktoren $p$ findes i $n!$ er saaledes

$$(6) \qquad q = \left(\frac{n}{p}\right) + \left(\frac{n}{p^2}\right) + \left(\frac{n}{p^3}\right) + \ldots$$

Vi ville give dette Udtryk en anden Form; skrives $n$ i $p$-Tal Systemet som

$$n = a_0 + a_1 p + a_2 p^2 + \ldots a_r p^r,$$

har man

$$\left(\frac{n}{p}\right) = a_1 + a_2 p + a_3 p^2 + \ldots + a_r p^{r-1},$$

$$\left(\frac{n}{p^2}\right) = \qquad a_2 \quad + a_3 p \quad \ldots + a_r p^{r-2},$$

$$\left(\frac{n}{p^3}\right) = \qquad a_3 \quad + \ldots + a_r p^{r-3},$$

..........................................

$$\left(\frac{n}{p^r}\right) = \qquad a_r,$$

*) Hvor Misforstaaelse kan finde Sted, sættes E (entier) foran Parentesen.



hvoraf ved Addition

$$(7)\ q = \frac{a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \ldots + a_r(p^r-1)}{p-1}$$

$$= \frac{n-t_n}{p-1},$$

hvor $t_n$ betyder Tværsummen af Tallet $n$, skrevet i $p$-Tal Systemet.

Heraf udledes for Binomialkoefficienterne

$$(8) \qquad \frac{(a+b)!}{a!\,b!} = \pi_p \frac{t_a + t_b - t_{a+b}}{p-1},$$

hvor Produktet kan udstrækkes til alle Primtal, da Eksponenten bliver Nul for $p > a + b$. Man ser let, at Eksponenten er lig det Antal Gange, man faar „Mente", naar $a$ og $b$, skrevne i det anvendte Talsystem, adderes.

Sætningen kan let udvides til Polynomialkoefficienterne.

Vi kunne mærke os, at *hvis Eksponenten er et Primtal, vil dette gaa op i alle de Koefficienter, der ikke ere 1.*

Vi ville undersøge, om denne Sætning ogsaa gælder for Binomialkoefficienterne naar Eksponenten ikke er et Primtal, med andre Ord om $n$ gaar op i

$$a_{n,q} = \frac{n(n-1)(n-2)\ldots(n-q+1)}{1 \cdot 2 \cdot 3 \ldots q}$$

Lad os borttage Faktoren $n$ i Tælleren og antage, at den Brøk, der bliver tilbage, er lig en uforkortelig Brøk med Nævneren $r$. Da nu Produktet af de $q$ første Tal gaar op i Produktet af $q$ paa hinanden følgende Tal, vil den uforkortelige Brøk gaa over til et helt Tal, hvis vi tilføje Faktoren $n-q$ i Tælleren eller borttage

Faktoren $q$ af Nævneren, altsaa baade ved Multiplikation med $n-q$ og med $q$. Dette er umuligt, hvis $q$ er pr. med $n$, medens det er muligt, naar $r$ er fælles Faktor for $n$ og $q$. Altsaa:

Binomialkoefficienten $a_{n,q}$ er delelig med $n$, naar $q$ er pr. med $n$, og med mindst $\frac{n}{r}$, naar $r$ er største fælles Faktor for $n$ og $q$.

10. *Catalan**) har ved Betragtning af elliptiske Funktioner fundet, at

$$\frac{(2\,a)!\,(2\,b)!}{a!\,(a+b)!\,b!}$$

altid er et helt Tal. Denne Sætnings Rigtighed følger af, at for ethvert Talsystem

$$t_a + t_{a+b} + t_b - t_{2a} - t_{2b}$$

ikke kan være negativ. For at vise dette, sætte vi

$$t_{2a} = 2t_a - \lambda;\; t_{2b} = 2t_b - \mu;\; t_{a+b} = t_a + t_b - \nu,$$

og vi skulle da vise, at

$$\lambda + \mu \geqq \nu,$$

hvor disse Tal betyde det Antal Gange, man faar „Mente" henholdsvis ved $a + a$, $b + b$ og $a + b$.

Er nu Grundtallet $g$ lige, kan man i $a + b$ kun faa „Mente", naar man adderer to Cifre, af hvilke mindst det ene er $\frac{1}{2}\,g$ eller større, men saa ville de samme Cifre give mindst een Gang „Mente" i $2a$ og $2b$. Er $g$ ulige, vil man i $a + b$ foruden i de nævnte Tilfælde

*) Nouv. annales 1874.



ogsaa faa „Mente", naar man adderer to Cifre $\frac{1}{2}\,(g-1)$, hvis man tilhøjre for disse træffer de samme Cifre 0, 1, 2... Gange og derpaa to Cifre, hvis Sum mindst er $g$. Man vil da imidlertid ogsaa faa „Mente" for det samme Ciffer enten i $2a$ eller i $2b$ eller i dem begge, og Sætningen er saaledes bevist for alle Tilfælde.

## Funktionen $\varphi\,(n)$.

11. Ved en talteoretisk Funktion forstaar man en saadan, som er defineret for alle hele Værdier af den variable. En saadan Funktion er $\varphi\,(n)$, der betegner Antallet af hele Tal, som er mindre end $n$ og primiske med $n$. (1 medregnet).

Om denne Funktion kunne vi bevise, at den har den i (3) udtrykte Egenskab, nemlig at

(9) $$\varphi\,(m)\;\varphi\,(n) = \varphi\,(mn),$$

naar $m$ og $n$ ere to indbyrdes primiske Tal.

For at bevise denne Sætning betragte vi Ligningen

$$mx + ny = a,$$

hvor vi for $x$ efterhaanden indsætte de $\varphi\,(n)$ Tal, der ere mindre end og pr. med $n$, for $y$ de $\varphi\,(m)$ Tal, der ere mindre end og pr. med $m$. Faa vi paa denne Maade en Værdi af $a$, der er større end $mn$, trække vi $mn$ fra den.

Vi have saaledes for $a$ faaet $\varphi\,(m)\;\varphi\,(n)$ Værdier, der ere mindre end $mn$ og som, da $m$ er pr. med $ny$ og $n$ med $mx$, ere pr. med $mn$. Vi kunne bevise, at de fundne Værdier alle ere forskellige; gav nemlig $mx + ny$ og $mx_1 + ny_1$ den samme Værdi, maatte

$$m\,(x - x_1) + n\,(y - y_1)$$

være delelig med $mn$, eller $m$ maatte gaa op i $y - y_1$, $n$ i $x - x_1$, hvad der er umuligt, da disse Differenser ikke begge kunne være Nul og henholdsvis ere mindre end $n$ og $m$. Vi have saaledes bestemt $\varphi(m)\,\varphi(n)$ Tal, der ere mindre end og pr. end $mn$, og af saadanne Tal gives der ingen andre; var nemlig $b$ et saadant Tal, vilde den ubestemte Ligning

$$mx + ny = b$$

bestemme et Værdipar $(x,y)$, hvor $x$ var mindre end og pr. med $n$, og $y$ mindre end og pr. med $m$, men alle saadanne Værdipar have vi benyttet. De fundne Tal ere saaledes netop alle de Tal, der ere mindre end og pr. med $mn$, og da disses Antal er $\varphi(mn)$, er vor Sætning bevist.

Er $p$ et Primtal, saa er alle Tal mindre end $p$ ogsaa pr. med $p$, saa at $\varphi(p) = p - 1$. Er Tallet $p^\alpha$, saa ere de Tal, der ere ikke større end og ikke pr. med $p^\alpha$

$$p,\ 2p,\ 3p, \ldots p^{\alpha-1}p,$$

i Antal $p^{\alpha-1}$; man har altsaa

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\,(1 - \frac{1}{p}).$$

Betragte vi nu et vilkaarligt Tal, opløst i Primfaktorer

$$n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_m^{\alpha_m},$$

have vi

$$\varphi(n) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_m^{\alpha_m})$$

eller

$$(10) \qquad \varphi(n) = n\,(1 - \frac{1}{p_1})\,(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_m}).$$



12. Vi ville udvikle denne Formel paa en anden Maade. De Tal, der ere mindre end $n$ og delelige med $p_1$, ere

$$p_1,\ 2p_1,\ 3p_1 \ldots \frac{n}{p_1} \cdot p_1,$$

i Antal $\frac{n}{p_1}$. Tilbage er der $n\left(1 - \frac{1}{p_1}\right)$ Tal, der ikke ere delelige med $p_1$; delelige med $p_2$ ere Tallene

$$p_2,\ 2p_2,\ 3p_2 \ldots \frac{n}{p_2} \cdot p_2,$$

men af disse er nogle delelige med $p_1$, nemlig de, hvor $p$ gaar op i Koefficienten til $p_2$; da Koefficienterne ere

$$1,\ 2,\ 3, \ldots \left(\frac{n}{p_2}\right),$$

ere $\frac{n}{p_2}\left(1 - \frac{1}{p_1}\right)$ delelige med $p_1$. Af Tal mindre end $n$, der hverken ere delelige med $p_1$ eller $p_2$, bliver der saaledes

$$\frac{n}{p_2} - \frac{n}{p_2}\left(1 - \frac{1}{p_1}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

og saaledes videre.

Hvis $n$ ikke er delelig med $p_1, p_2, \ldots$ giver (10) ikke nogen brugbar Tilnærmelsesformel for Antallet af Tal, der ere mindre end $n$ og ikke delelige med $p_1, p_2 \ldots$, da den mulige Fejl vokser meget stærkt med Antallet af Primtallene.

13. Da Funktionen $\varphi$ tilfredsstiller Betingelsen (9), kunne vi i (2) og det udviklede Produkt for ethvert Led $l$ sætte $\varphi(l)$.

Vi faa derved for en af Parenteserne $(1 + p + p^2 + \ldots p^\alpha)$

$$1 + p - 1 + p\,(p-1) + p^{\alpha-1}\,(p-1) = p^\alpha$$

og derfor for hele Produktet netop selve Tallet $n$. I det udviklede Produkt have vi Summen af Divisorerne og vi faa saaledes Formlen, (hvor 1, $d_1$, $d_2$ ... ere Divisorerne)

$$(11) \qquad 1 + \varphi(d_1) + \varphi(d_2) + \varphi(d_3) \ldots + \varphi(n) = n.$$

14. Formlen (11) kan ogsaa udledes saaledes:

Vi betragte alle de Tal, som ere mindre end $n$ og som med $n$ har en af Divisorerne $d$ til største fælles Maal. Dividere vi disse Tal med $d$, faa vi de Tal, der ere mindre end $\frac{n}{d}$ og pr. med dette Tal, i Antal $\varphi\left(\frac{n}{d}\right)$. Gentager man dette for alle Divisorerne, maa man have faaet alle Tallene 1, 2, 3, ... $n$ hvert netop een Gang, da et Tal ikke med $n$ kan have flere end et største fælles Maal. Man har altsaa

$$\varphi\left(\frac{n}{1}\right) + \varphi\left(\frac{n}{d_1}\right) + \varphi\left(\frac{n}{d_2}\right) + \ldots \varphi\left(\frac{n}{n}\right) = n,$$

men denne Løsning er i Virkeligheden den samme som (11), da man ved at dividere et Tal med alle dets Divisorer atter faar alle dets Divisorer.

## Funktionen $\mu$ $(n)$.

15. *Møbius* har ved nogle Undersøgelser*) til ethvert Tal i Talrækken knyttet et af Tallene —1, 0, + 1 efter følgende Regel:

Til ethvert Tal, der er deleligt med et Kvadrattal, hører Tallet 0, medens —1 og + 1 henholdsvis hører til Tal med et ulige og med et lige Antal Primfaktorer.

*) Crelles Journal Bd. 9 Pg. 105.



Vi betegne det til $n$ hørende Tal ved $\mu(n)$ eller, hvor det ikke kan misforstaas, blot ved $\mu$. Vi have saaledes

$$\mu(1) = 1;\ \mu(2) = -1;\ \mu(3) = -1;\ \mu(4) + 0;\ \mu(5) = -1;$$
$$\mu(6) = +1;\ \mu(7) = -1;\ \mu(8) = \mu(9) = 0;\ \mu(10) = +1;$$
$$\mu(11) = -1;\ \mu(12) = 0 \text{ o. s. v.}$$

16. Af Definitionen følger, at for de to indbyrdes primiske Tal, $m$ og $n$, er

$$\mu(m)\ \mu(n) = \mu(mn),$$

og vi kunne derfor i (2) for ethvert Led $l$ sætte $\mu(l)$; derved faar vi for enhver af Parenteserne $1—1+\ldots = 0$, saa at man for et vilkaarligt Tal har

$$(12) \qquad \Sigma\ \mu(d) = 0,$$

hvor Summationen udstrækkes til alle Tallets Divisorer. Vi have altsaa Sætningen:

Summen af alle til et Tals Divisorer hørende Møbius' Faktorer er Nul.

17. Dersom vi i 2 for ethvert Led $l$ sætte $\frac{\mu(l)}{l}$, der tilfredsstiller Betingelsen, bliver enhver af Parenteserne til $1 - \frac{1}{p}$; idet Produktet af disse Størrelser i Følge (10) er $\varphi(n) : n$, have vi saaledes

$$(13) \qquad \Sigma\ \mu(d)\frac{1}{d} = \frac{\varphi(n)}{n}$$

18. Dersom vi udvikle Produktet

$$(1-p_1)\ (1-p_2) \ldots (1-p_n),$$

faa vi Summen af alle Tallets Divisorer, enhver multipliceret med sit $\alpha$. De Led, der indeholde $p$, ere

$$-p_1\,(1-p_2)\,(1-p_3)\ldots(1-p_n),$$

og af disse Led er der, naar Tallet har andre Primfaktorer end $p$, lige mange positive og negative. Da dette gælder for enhver af Tallets Primfaktorer, har man:

Produktet af de af et Tals Divisorer, hvis $\mu$ er $+1$, er lig Produktet af de Divisorer, hvis $\mu$ er $-1$, naar Tallet ikke er en Potens at et Primtal.

19. Sætningen kan ogsaa udtrykkes ved Ligningen

$$(14) \qquad \Sigma\,\mu(d) l.d = 0.$$

der gælder for ethvert Tal, der ikke er Potens af et Primtal.

Ved Hjælp heraf kunne vi se Betydningen af Udtrykket

$$(15)\quad f(x) = l.2\left(\frac{1}{l.2}+\frac{1}{l.4}+\frac{1}{l.6}+\ldots\right)+l.3\left(\frac{1}{l.3}+\frac{1}{l.6}+\right)$$
$$+\ldots+\mu(n) l.n\left(\frac{1}{ln}+\frac{1}{l.2n}+\ldots\right),$$

hvor vi overalt fortsætte saa længe, som Tallene under Logaritmetegnene ere mindre end et givet Tal $x$ (som vi tænke os ikke helt). Vi se nu, at alle de Led, i hvis Nævner der findes $l.a$, hvor $a$ er et Tal med forskellige Primfaktorer, hæve hinanden. Saaledes forekommer f. Eks. $l.30$ $(30 < x)$ i de Rækker, der ere multiplicerede med $l.2$, $l.3$, $l.5$, $-l.6$, $-l.10$, $-l.15$, $-l.30$, hvis Sum i Følge (14) er Nul. For et Primtal faa vi kun et Led



$$l.p\,\frac{1}{l.p} = 1;$$

for et Primtalskvadrat faa vi

$$l.p\,\frac{1}{l.p^2} = \frac{1}{2}$$

og saaledes videre.

$f(x)$ er altsaa Antallet af Primtal, mindre end $x$ + det halve Antal Primtalskvadrater, mindre end $x$ + Trediedelen af Primtalskuber, mindre end $x$ o. s. v.

20. Man har ofte Brug for Ligningen

$$(16)\quad \left(\frac{a}{1}\right)-\left(\frac{a}{2}\right)-\left(\frac{a}{3}\right)-\left(\frac{a}{5}\right)+\left(\frac{a}{6}\right)+\ldots$$
$$+\mu(n)\left(\frac{a}{n}\right)+\ldots+\left(\frac{a}{a}\right)=1,$$

hvor $a$ er et vilkaarligt helt Tal. Beviset føres let ved Induktion. Sætningen gælder for $a = 1$, og vi skulle derfor blot vise, at hvis den gælder for $a$, gælder den ogsaa for $a+1$. Sætte vi $a+1$ for $a$, blive alle Leddene uforandrede undtagen de Led, hvor Nævneren er Divisor i $a+1$; er en saadan Divisor $d$, bliver der til Leddets Værdi adderet $\mu(d)$, og da i Følge 16 $\Sigma\,\mu(d) = 0$, er Sætningen bevist.

21. Vi ville benytte dette til at bevise, at mindste fælles Multiplum $M$ for Tallene 1, 2, 3 ... $n$ er

$$(17)\qquad M = \frac{n\,!\left(\frac{n}{6}\right)!\left(\frac{n}{10}\right)!\ldots}{\left(\frac{n}{2}\right)!\left(\frac{n}{3}\right)!\left(\frac{n}{5}\right)!\ldots}$$

hvor Brøkerne i Tælleren til Nævnere have de Tal, hvis $\mu$ er $+1$, i Nævneren de, hvis $\mu$ er $-1$, og hvor man begge Steder fortsætter saa længe, til Faktorerne faa Værdien 1.

I det mindste fælles Multiplum for Tallene $1, 2, 3 \ldots n$, findes de Primfaktorer een Gang, som ligge mellem $n$ (inklusive) og $\sqrt{n}$ de to Gange, som ligge mellem $\sqrt{n}$ og $\sqrt[3]{n}$ o. s. v. Vi skulle derfor vise, at de netop findes saa mange Gange i (17).

Er $n \gtreqqless p > \sqrt{n}$ vil $n$ skrevet i $p$-Tal Systemet have Formen $ap + l$, og det Antal Gange $p$ findes i $n$ er $\left(\frac{n}{p}\right) = a$. Endvidere er $\frac{n}{q} = \left(\frac{a}{q}\right) p + \ldots$, saa at $p$ findes $\left(\frac{a}{q}\right)$ Gange i $\left(\frac{n}{q}\right)!$. Det hele Antal Gange $p$ findes i Brøken (17) er derfor

$$a - \left(\frac{a}{2}\right) - \left(\frac{a}{3}\right) - \left(\frac{a}{5}\right) + \left(\frac{a}{6}\right) \ldots + \left(\frac{a}{a}\right) = 1,$$

stemmende med det, vi skulde bevise.

Ligger $p$ mellem $\sqrt{n}$ og $\sqrt[3]{n}$ har man $n = ap^2 + bp + c$, og det Antal Gange $p$ findes i $n!$ er

$$\left(\frac{n}{p^2}\right) + \left(\frac{n}{p}\right) = a + a_1 \; (a_1 = ap + b).$$

Idet man danner de analoge Udtryk for alle Faktorer og Divisorer i (17), faar man den søgte Eksponent som en Sum af to Rækker, den ene den samme som ovenfor, og den anden dannet deraf ved at sætte $a_1$ for $a$. Da begge Rækker have Summen 1, er den fundne Eksponent 2, som det skulde bevises. Paa samme Maade kunne vi fortsætte, til Formlens Rigtighed er bevist.

Man kan ikke finde Tilnærmelsesværdien for $M$ ved



at afbryde Tæller og Nævner i Brøken, da man ikke, uafhængigt af Tallenes Opløsning i Primfaktorer, kender den Lov, efter hvilken Talrækkens $\mu$-Faktorer følger efter hinanden; vi skulle senere se, hvorledes det er lykkedes for *Thebychef* at finde Grænser for M.

Et andet Udtryk for mindste fælles Multiplum er

$$\text{(18)} \qquad M = \frac{2^{\left(\frac{n}{2}\right)} \cdot 3^{\left(\frac{n}{3}\right)} \cdot 5^{\left(\frac{n}{5}\right)} \cdots}{6^{\left(\frac{n}{6}\right)} \cdot 10^{\left(\frac{n}{10}\right)} \cdot 14^{\left(\frac{n}{14}\right)} \cdots},$$

hvis Sammensætning er i Øjne faldende. Man ser, at Eksponenten til en Primfaktor f. Eks. 2 bliver

$$\left(\frac{n}{2}\right) - \left(\frac{n}{6}\right) - \left(\frac{n}{10}\right) - \left(\frac{n}{14}\right) - \left(\frac{n}{22}\right) - \left(\frac{n}{26}\right) + \left(\frac{n}{30}\right) - \ldots$$

Dette Tal er netop Eksponenten til den højeste Potens af 2, der findes mellem Tallene $1, 2, 3 \ldots n$; det forandres nemlig ikke, naar $n$ vokser, undtagen, naar $n$ passerer en Potens af 2, da det vokser med en Enhed, og for $n = 2$ er det 1.

22. *Møbius* har benyttet de nævnte Faktorer til Omvending af visse Rækker. Kan man nemlig af en Række

$$y_1 = x_1 + x_2 + x_3 + x_4 + \ldots$$

danne de ny Rækker

$$\text{(19)} \qquad \begin{aligned} y_2 &= x_2 + x_4 + x_6 + x_8 + \ldots \\ y_3 &= x_3 + x_6 + x_9 + x_{12} + \ldots \\ y_4 &= x_4 + x_8 + x_{12} + x_{16} + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

og multiplicerer man enhver Række $y_n$ med $\mu(n)$, faar man ved Addition

$$(20) \qquad x_1 = y_1 - y_2 - y_3 - y_5 + y_6 \ldots + \mu_n y_n + \ldots$$

idet ethvert andet $x$ ved Additionen falder bort, da man faar det multipliceret med Summen af dets Mærketals Divisorers $\mu$-Faktorer, en Sum, der ifølge 16 er Nul. Rækkerne forudsættes konvergente.

Have vi saaledes den for $|x| < 1$ konvergente Række

$$y_1 = \frac{x}{1-x} = x + x^2 + x^3 + \ldots,$$

danne vi deraf de andre konvergente Rækker, idet vi for $x$ sætte $x^2, x^3, \ldots$ Vi faa saaledes

$$x = \frac{x}{1-x} - \frac{x^2}{1-x^2} - \frac{x^3}{1-x^3} \ldots + \mu(n) \frac{x^n}{1-x^n} + \ldots$$

eller ved en lille Ændring

$$1 - x = 1 - \frac{x}{1+x} - \frac{x^2}{1+x+x^2} - \ldots + \mu(n) \frac{x^n}{1+x+x^2+\ldots x^n} + \ldots,$$

gældende for $|x| < 1$.

Møbius har heraf, ved at sætte $x = 1$, udledt Relationen

$$1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{6} + \ldots + \mu(n) \frac{1}{n} + \ldots = 0,$$

men dette Bevis er ikke gyldigt, da det ikke er bevist, at Rækken er konvergent for $x = 1$. Nærmere kommer man, naar man i (16) for $\left(\frac{a}{n}\right)$ sætter $\frac{a}{n} - \varepsilon_n$, hvor $\varepsilon_n$ er en ægte, positiv Brøk. Man faar da efter Division med $a$, naar man lader $a$ vokse i det uendelige,

$$\Sigma \mu(n) \frac{1}{n} = \frac{\Sigma \mu(n) \varepsilon_n}{a} \; (a = \infty),$$



hvor Størrelsen paa højre Side i alt Fald maa ligge mellem $-1$ og $+1$.

En anden Række, som Møbius anvender, er

$$-l.(1-x) = x + \frac{1}{2} x^2 + \frac{1}{3} x^3 + \ldots + \frac{1}{n} x^n + \ldots,$$

hvoraf man faar

$$x = -l.(1-x) + \frac{1}{2} l.(1-x^2) + \frac{1}{3} l.(1-x^3) + \ldots$$

$$- \mu(n) \frac{1}{n} l.(1-x^n) + \ldots$$

$$= -l.(1-x).(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{6} \ldots) + \frac{1}{2} l.(1+x)$$

$$+ \frac{1}{3} l.(1+x+x^2) + \ldots$$

der gælder for $|x| < 1$, men som ogsaa anvendes af Møbius for $x = 1$, hvorved

$$\frac{1}{2} l.2 + \frac{1}{3} l.3 + \frac{1}{5} l.5 - \frac{1}{6} l.6 + \ldots = 1,$$

en Formel hvis Rigtighed ligesom den forriges er tvivlsom.

23. Lad os antage, at vi i (19) standse ved Index $n$ og saaledes faa $n$ lineære Ligninger med $n$ ubekendte. Ligningernes Determinant er

$$(21) \qquad D = \left\{ \begin{matrix} 1&1&1&1&1&1&1&1&1&1&\ldots \\ 0&1&0&1&0&1&0&1&0&1&\ldots \\ 0&0&1&0&0&1&0&0&1&0&\ldots \\ 0&0&0&1&0&0&0&1&0&0&\ldots \\ 0&0&0&0&1&0&0&0&0&1&\ldots \\ 0&0&0&0&0&1&0&0&0&0&\ldots \\ 0&0&0&0&0&0&1&0&0&0&\ldots \\ 0&0&0&0&0&0&0&1&0&0&\ldots \\ 0&0&0&0&0&0&0&0&1&0&\ldots \\ 0&0&0&0&0&0&0&0&0&1&\ldots \\ \ldots&&&&&&&&&&\ldots \\ \ldots&&&&&&&&&&\ldots \end{matrix} \right\} = 1,$$

en Determinant, der har flere mærkelige talteoretiske Egenskaber. Dens Værdi er 1, da alle dens Led ere Nul undtagen Diagonalleddet.

Af Ettaller forekommer der i $m$te Række $\left(\frac{n}{m}\right)$, i $m$te Søjle $d_m$, idet vi herved forstaa Antallet af Divisorer i $m$. Heraf følger da, idet man maa faa samme Antal ved at summere efter Rækker som ved at summere efter Søjler

$$(22)\left(\frac{n}{1}\right)+\left(\frac{n}{2}\right)+\left(\frac{n}{3}\right)+\ldots+\left(\frac{n}{n}\right)=1+d_2+d_3+\ldots+d_n.$$

Lad $A_m$ være Underdeterminanten til det første Element af den $m$te Række; vi faa da, idet vi multiplicere den første Søjles Underdeterminanter med Elementerne af første, anden, tredie ... Søjle og adderer

$$A_1 = 1,\ A_1 + A_2 = 0;\ A_1 + A_3 = 0;\ A_1 + A_2 + A_4 = 0,$$
$$A_1 + A_5 = 0\ldots,$$

hvor Indices i enhver af Ligningerne ere den sidstes Divisorer; deraf følger, at Ligningerne ere tilfredsstillede af $A_m = \mu(m)$, og da de bestemme de ubekendte entydig, er der ingen anden Løsning. Vi se saaledes, at:

Den første Søjles Underdeterminanter ere de tilsvarende Nummertals $\mu$-Faktorer.

Vi faa herved, idet vi opløse efter den første Søjle efter til den at have adderet alle de andre,

$$\Sigma\,\mu(m)\left(\frac{n}{m}\right)=1,$$

stemmende med (16).



24. Søge vi Underdeterminanterne $B_i$ til den $m$te Søjles Elementer, se vi, ved at kombinere dem som ovenfor med de foregaaende Søjlers og den $m$te Søjles Elementer, at de alle ere Nul til $B_m$, der er 1 og ved at kombinere dem de efterfølgende Søjlers Elementer, at $B_r$ er Nul i alle Tilfælde, hvor $r$ ikke er et Multiplum af $m$, og vi faa til disses Bestemmelse, naar vi udelade Faktoren $m$ i Indices, de samme Ligninger, der tidligere tjente til Bestemmelse af den første Søjles Underdeterminanter; altsaa er

$$(23)\qquad B_{mk} = \mu(k).$$

25. Af $D$ kunne vi danne en anden Determinant $D_n$, idet vi for ethvert Element sætte dets Underdeterminant,

$$(24)\quad D_1 = \left\{\begin{array}{rrrrrrrrrl}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
-1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \ldots \\
-1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\
+1 & -1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots \\
-1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \ldots \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & \ldots \\
. & . & . & . & . & . & . & . & . & \ldots \\
. & . & . & . & . & . & . & . & . & \ldots
\end{array}\right\} = 1.$$

Ifølge bekendte Sætninger i Determinantteorien har man $D_1 = 1$, medens Underdeterminanterne i $D_1$ ere de tilsvarende Elementer i $D$.

Addere vi de øvrige Rækker til den første og opløse

vi derpaa efter denne, faa vi, idet $\Sigma\mu(n)$ betegner Summen $\mu(1) + \mu(2) \ldots + \mu(n)$

$$(25) \quad \Sigma\mu(n) + \Sigma\mu\left(\frac{n}{2}\right) + \Sigma\mu\left(\frac{n}{3}\right) + \ldots + \Sigma\mu\left(\frac{n}{n}\right) = 1.$$

Denne Ligning kan tjene som Definition for $\Sigma\mu(n)$, thi indsætter man for $n$ efterhaanden $\frac{n}{2}, \frac{n}{3} \ldots$, og anvender man Møbius' Fremgangsmaade, finder man det kendte Udtryk for $\Sigma\mu(n)$.

---

# ANDET KAPITEL

## OM KONGRUENSER

### Kongruenser af første Grad.

26. Ved at $a$ er kongruent med $b$ for Modulus $n$, der skrives

$$(1) \quad a \equiv b \pmod{n},$$

forstaa vi, at $a$ og $b$ give samme Rester ved Divivion med $n$ eller, at $n$ gaar op i $a—b$. Den ubestemte Ligning

$$(2) \quad ax - ny = b$$

kan derved skrives

$$(3) \quad ax \equiv b \pmod{n}$$

der kaldes Kongruensen af første Grad.

Kongruensbegrebet kan udvides til Brøker; ved

$$\frac{a}{b} \equiv c \pmod{n},$$

hvor $a$ og $b$ ere indbyrdes pr., forstaa vi da, at det hele Tal, som vi faa, naar vi til Brøkens Tæller addere et passende Multiplum af $n$, er lig med $c$. Paa lignende Maade kunne vi udvide Begrebet til Rodstørrelser, idet vi f. Eks. ved

$$\sqrt{-1} \equiv x \pmod{n}$$

forstaa Rødderne i Kongruensen

$$x^2 + 1 \equiv 0 \pmod{n}$$

En Kongruens kan opfattes som en Ligning, naar vi vedtage at regne alle Tal, der give samme mindste Rest ved Division med Modulus som eet Tal. Dele vi en Cirkelperiferi i $n$ lige store Dele, og mærke vi alle Delingspunkterne i Orden med Tallene .... —2, —1, 0, 1, 2..., blive altsaa alle Tal, der mærke det samme Punkt, at regne som ensgældende for Modulus $n$. En Kongruens kan derfor skrives som en Ligning, naar man paa den ene Side tilføjer et Led, der er et ubestemt Multiplum af Modulus; omvendt kunne vi af en Ligning mellem hele Tal danne en Kongruens for en vis Modulus, idet vi for ethvert Leds Faktorer sætte deres Rester og ombytte = med $\equiv$.

27. Hvis i (2) $a$ og $n$ ere indbyrdes pr., ville som bekendt alle Værdierne af $x$ danne en Differensrække med Differensen $n$. Da alle disse Tal ere ensgældende, naar vi betragte Kongruensen (3), sige vi, at denne har een Løsning, altsaa

Kongruensen (3) har altid een og kun een Løsning, naar $a$ er pr. med $n$.

Hvis $f$ er største fælles Faktor for $a$ og $n$, faa vi af (2)

$$\frac{a}{f}\,x - \frac{n}{f}\,y = \frac{b}{f},$$

altsaa

$$\frac{a}{f}\,x \equiv \frac{b}{f} \left(\text{mod.}\ \frac{n}{f}\right),$$

hvoraf vi udlede Sætningen:



Har i (3) $a$ og $n$ en fælles Faktor, maa denne ogsaa være i $b$, hvis Kongruensen skal være mulig; er dette Tilfældet, kan den bortdivideres af $a$ og $b$, men den maa da ogsaa bortdivideres af Modulus.

I dette Tilfælde danne Løsningerne en Differensrække med Differensen $\frac{n}{f}$, og vi maa derfor, dersom vi fastholde $n$ som Modulus for Kongruensen, sige, at denne har $f$ Rødder.

28. Vi ville anvende det foregaaende til Løsning af følgende Opgave:

Find et Tal, der ved Division med $n$ og $m$ giver Resterne $\alpha$ og $\beta$.

Det søgte Tal har Formerne $yn + \alpha$ og $xm + \beta$, saa at

$$xm \equiv (\alpha - \beta) \pmod{n}, \tag{4}$$

Vi se heraf, at Opgaven er umulig, dersom $m$ og $n$ har en fælles Faktor, der ikke findes i $\alpha - \beta$. Er $f$ største fælles Faktor for $m$ og $n$ og $\alpha - \beta = kf$, faas naar $x_1$ er en Løsning af Kongruensen,

$$x = x_1 + h\frac{n}{f},$$

hvor $h$ er et helt Tal, og deraf det søgte Tal

$$mx_1 + \beta + h.\frac{mn}{f}, \tag{5}$$

der viser, at alle Løsningerne danner en Differensrække, hvis Differens er mindste fælles Multiplum for de givne Divisorer. Denne Sætning gælder ogsaa, hvis der er givet flere Divisorer og de tilsvarende Rester.

29. En anden Opgave er følgende:

At dele en ægte, uforkortelig Brøk med Nævneren $ab$, hvor $a$ og $b$ ere indbyrdes pr., i to andre med Nævnerne $a$ og $b$.

Man skal altsaa have

$$\frac{m}{ab} = \frac{x}{a} + \frac{y}{b} \text{ eller } bx + ay = m. \ (m \text{ pr. med } a \text{ og } b \text{ og } < ab)$$

Løsningerne af denne Ligning have Formen

$$x = \alpha + ka, \ y = \beta + lb,$$

hvor $\alpha$ og $\beta$ ere positive Tal, henholdsvis mindre end $a$ og $b$, medens $k$ og $l$ ere hele Tal med en bestemt Sum, men forøvrigt vilkaarlige; vi faa nu

$$\frac{m}{ab} = \frac{\alpha}{a} + \frac{\beta}{b} + k + l,$$

hvor de to Brøkers Sum ligger mellem 0 og 2, saa at maa have $k + l = 0$ eller $k + l = -1$. I det sidste Tilfælde kan man sætte

$$\frac{m}{ab} = \frac{\alpha}{a} - \frac{b-\beta}{b} = \frac{\beta}{b} - \frac{\alpha - a}{a} \tag{6}$$

Vi se saaledes, at

En uforkortelig, ægte Brøk med Nævneren $ab$, hvor $a$ og $b$ ere indbyrdes primiske, kan enten skrives paa een Maade som en Sum af to ægte Brøker med Nævnerne $a$ og $b$ eller paa to Maader som en Differens af to saadanne Brøker.

Ere $a$ og $b$ ikke Primtal eller Potenser af saadanne, kan Dekompositionen fortsættes paa samme Maade, saaledes faar man



$$\frac{m}{2.3.5.7\ldots p} = \frac{\alpha}{2} + \frac{\beta}{3} + \frac{\gamma}{5} + \frac{\delta}{7} + \ldots + \frac{\mu}{p}$$

hvor Tællerne ere positive eller negative hele Tal, numerisk mindre end de tilsvarende Nævnere. Kan man paa den anden Side finde saadanne Værdier af Tællerne, at man faar en Værdi af $m$, der er mindre end $p^2$, da maa $m$ være et Primtal.

## Fermats og Wilsons Sætninger.

30. Lad

$$1, a_1, a_2, a_3 \ldots a_r$$

være de $\varphi(n)$ Tal, der ere mindre end $n$ og pr. med $n$ og $a$ et vilkaarligt af dem. Af Tallene

$$a, a_1 a, a_2 a, \ldots a_r a$$

er intet deleligt med $n$. Differensen mellem to af dem er heller ikke delelig med $n$, da den har Formen $ka$, hvor $k < n$ og $a$ pr. med $n$. Tallene i Rækken maa derfor give forskellige mindste Rester med $n$, og da disse Rester maa være pr. med $n$, maa de bestaa af Tallene 1, $a_1 a_2 \ldots a_r$ i en eller anden Orden; man har derfor

$$a_1 \, a_2 \ldots a_r \, a^{\varphi(n)} \equiv a_1 \, a_2 \ldots a_r \text{ mod } n.$$

eller

$$a_1 \, a_2 \ldots a_r \, (a^{\varphi(n)} - 1) \equiv 0 \text{ (mod. } n).$$

$n$ gaar altsaa op i Produktet paa venstre Side, og da $n$ er pr. med $a_1 \, a_2 \ldots a_r$, følger heraf

Naar $a$ er primisk med $n$, gaar $n$ op i $a^{\varphi(n)} - 1$,

og specielt

Et Primtal $p$, som ikke gaar op i $a$, gaar op i $a^{p-1}-1$.

Det er i dette specielle Tilfælde, at Sætningen er opstillet uden Bevis af *Fermat*; den bevistes og udvidedes til den almindelige Sætning (den udvidede Fermatske Sætning) af *Euler*.

31. Et andet simpelt Bevis for den Fermatske Sætning faar man ved at erindre, at man ved at udvikle $(a+1)^p$ efter Binomialformlen, faar lutter Led, der ere delelige med $p$, undtagen det første og det sidste, man har derfor for Modolus $p$, hvor $p$ er et Primtal,

$$(a+1)^p \equiv a^p + 1 \equiv (a-1)^p + 2 \equiv (a-2)^p \dots + 3 \equiv a + 1,$$

en Form, i hvilken Sætningen ogsaa gælder, naar $a+1$ er delelig med $p$.

32. Danner man Permutationer med Gentagelser af $a$ Elementer til $p$, er Antallet som bekendt $a^p$. Af disse bestaa $a$ af lutter ens Elementer, medens de øvrige kunne ordnes i Grupper med $p$ i hver, saaledes at de, der høre til samme Gruppe, dannes af en af dem ved Kredsforskydning; vi have saaledes her et nyt Bevis for, at $a^p - a$ er delelig med $p$.

33. Den ubestemte Ligning af første Grad løses som bekendt i Almindelighed ved Hjælp af Kædebrøk; ved Hjælp af Fermats Sætning faar man en explicit Løsning, der imidlertid i Reglen er et saa stort Tal, at det er ubekvemt i Praksis.

Af $ax \equiv b$ (mod. $n$) faar man ved Multiplikation med $a^{\varphi(n)-1}$

$$x \equiv b a^{\varphi(n)-1} \text{ (mod. } n).$$



34. Vi ville som Anvendelse af Fermats Sætning bevise en Sætning, som vi faa Brug for senere. Lad

$$(7) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n = (x-x_1)(x-x_2)\dots(x-x_n) = 0$$

være en algebraisk Ligning af $n$te Grad med hele Koefficienter og med Rødderne $x_1\ x_2 \dots x_n$. Vi ville opløfte paa begge Sider til $p$de Potens, hvor $p$ er et ulige Primtal. Paa venstre Side faa vi

$$(8) \qquad x^{np} + a_1^p\, x^{(n-1)p} \dots + a_n^p + pA,$$

hvor $A$ er et Polynomium med hele Koefficienter, hvis Leds Eksponenter kunne være eller ikke være delelige med $p$.

Paa den anden Side sætte vi

$$(9) \qquad (x-x_k)^p = x^p - x_k^p - p\left((x^{p-1}x_k - \frac{p-1}{2}x^{p-2}x_k^2 + \dots\right),$$

saa at Produktet bliver

$$(10) \qquad (x^p - x_1^p)(x^p - x_2^p)\dots(x^p - x_n^p) + pB.$$

hvor $B$ er et Polynomium, hvis Koefficienter ere symmetriske Funktioner af Rødderne og derfor kan udtrykkes uden Brøk ved $a_1,\ a_2 \dots a_n$. Det samme gælder om det første Led, hvor vi dog kun faa saadanne Eksponenter for $x$, der ere delelige med $p$. Vi have saaledes faaet to identiske Udtryk, og vi maa atter faa en Identitet, hvis vi af dem begge kun benytte de Led, hvis Eksponenter ere delelige med $p$, og heri overalt sætte $x$ for $x^p$; vi faa derved

$$(11)\quad x^n + a_1^p x^{n-1} + a_2^p x^{n-2} \ldots + a_n^p \equiv (x - x_1^p)(x - x_2^p) \ldots (x - x_n^p) \text{ (mod. } p).$$

Da nu i Følge Fermats Sætning $a^p \equiv a$ (mod. $p$), have vi Sætningen:

D e r s o m v i a f e n L i g n i n g, h v i s K o e f f i c i e n - t e r e r e h e l e T a l, d e n f ø r s t e l i g 1, d a n n e d e n L i g n i n g, h v i s R ø d d e r e r e d e $p$ d e P o t e n s e r a f d e n f ø r s t e s, d a e r e d e t o L i g n i n g e r s K o e f f i c i - e n t e r p a r v i s k o n g r u e n t e f o r M o d u l u s $p$.

35. Vi dele en Cirkelperiferi i $p$ lige store Dele og danne alle mulige $p$-Kanter (egentlige og uegentlige), som have deres Vinkelspidser i Delingspunkterne, idet vi begynde ved et bestemt Delingspunkt og bemærke, at hver Polygon kan beskrives i to Omløbsretninger, se vi, at Antallet af Polygoner er $\frac{1}{2}(p-1)!$ Af disse ere $\frac{1}{2}(p-1)$ regelmæssige, idet de ikke forandres ved at at drejes $\frac{1}{p}$ af en Omdrejning om Centrum. De øvrige danne Grupper af $p$ kongruente, der dannes af hinanden ved de nævnte Drejninger. $p$ maa altsaa gaa op i

$$\frac{1}{2}(p-1)((p-2)!-1),$$

og altsaa i den sidste Faktor; ved Multiplikation af denne med $p-1$, faar man da d e n W i l s o n s k e S æ t - n i n g:

N a a r $p$ e r e t P r i m t a l, g a a r $p$ o p i $(p-1)! + 1$.

Denne Egenskab findes kun ved Primtallene; man ser nemlig let, at et sammensat Tal $n$ ($> 4$) altid gaar op i $(n-1)!$



36. Ogsaa Wilsons Sætning kan udvides til sammensatte Tal; lad $n$ være et saadant og

$$1,\ a_1,\ a_2 \ldots a_r$$

være de $\varphi(n)$ Tal, der ere mindre end og pr. med $n$. Lad $a_m$ være Løsningen af Kongruensen

$$(12)\qquad a_s x \equiv 1 \text{ (mod. } n),$$

saa at $a_s . a_m \equiv 1$ (mod $n$). Vi se saaledes, at Tallene $a$ kunne parres to og to, saaledes at Produktet af to parrede er $\equiv 1$; herfra undtages dog de Tilfælde, hvor $a_m = a_s$, det vil sige de Tal, der tilfredsstille Kongruensen

$$(13)\qquad x^2 \equiv 1 \text{ (mod. } n).$$

Sætte vi nu

$$(14)\qquad 1 . a_1 a_2 \ldots a_r \equiv y \text{ (mod. } n)$$

kunne vi ved Bestemmelse af $y$ udelade de parrede Tal, saa at vi kun benytte de af Tallene $a$, der ere Rødder i (13). Disse kunne ogsaa parres, idet til en Rod $x$ svarer en anden $n - x$, der er forskellig fra $x$ undtagen for $x = \frac{1}{2} n$, et Tal, der imidlertid (bortset fra $n = 2$) ikke er pr. med $n$. Produktet af to parrede Rødder er nu

$$x(n - x) \equiv -x^2 \equiv -1 \text{ (mod. } n).$$

Vi have saaledes

$$y = (-1)^{\varrho},$$

hvor $\varrho$ er Antallet af Rodpar i Kongruensen (13). I denne, d e n u d v i d e d e W i l s o n s k e S æ t n i n g er den specielle indbefattet.

Kongruensen (13) vil senere blive nærmere undersøgt.

## Kongruenser af højere Grad.

37. Om Kongruenser af højere Grad er der ikke meget at sige i Almindelighed; kun naar Modulus er et Primtal, indtræder der visse Analogier med algebraiske Ligninger. Vi ville derfor foreløbig nøjes med at betragte dette Tilfælde.

Kongruensen af $n$te Grad med Primtalsmodulus har Formen

(15) $$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n \text{ (mod. } p),$$

hvor Koefficienterne ere hele Tal; som vi kunne forudsætte positive og mindre end $p$; de kunne være Nul med Undtagelse af $a_0$.

Vi kunne altid ændre Kongruensen saaledes, at den første Koefficient bliver 1, idet vi multiplicere med et Tal $y$, bestemt ved Kongruensen

$$a_0 y \equiv 1. \text{ (mod. } p).$$

38. Kongruensen af $n$te Grad har højst $n$ Rødder.

Er Kongruensen

(16) $$f(x) \equiv 0, \text{ (mod. } p),$$

og er $\alpha_1$ Rod (som vi kunne tænke os mindre end $p$), kunne vi sætte

$$f(x) = (x - \alpha_1)\, Q + R \equiv 0 \text{ (mod. } p),$$

hvor $Q$ er et helt Polynomium af Graden $n-1$, og $R$ er et helt Tal. Da $f(x)$ er delelig med $p$ for $x = \alpha_1$, maa $p$ gaa op i $R$, og vi kunne derfor sætte

$$f(x) \equiv (x - \alpha_1)\, Q. \text{ (mod. } p).$$



Er nu $\alpha_2$ en anden Rod, skal $p$ gaa op i $(\alpha_2 - \alpha_1)\, Q_{\alpha_2}$, hvor $Q_{\alpha_2}$ er Værdien af $Q$ for $x = \alpha_2$; da nu $\alpha_2$ og $\alpha_1$ ikke ere kongruente, maa $p$ gaa op i $Q_{\alpha_2}$, saa at man kan sætte

$$Q = (x - \alpha_2)\, Q_1$$

eller

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2)\, Q_1,$$

hvor $Q_1$ er af Graden $n - 2$. Idet vi fortsætte paa denne Maade, kan der indtræffe to Tilfælde; vi komme tilsidst til en Kongruens af første Grad, der, som vi vide, har een Rod; i dette Tilfælde har den givne Kongruens $n$ Rødder, men vi kunne ogsaa komme til en Kongruens af højere end første Grad uden Rødder; vi have nemlig selv for Primtalsmodulus ikke nogen Sætning, der svarer til Algebraens Fundamentalsætning, at enhver algebraisk Ligning har mindst een Rod. Saaledes har Kongruensen

$$x^2 + x + 1 \equiv 0 \text{ (mod. 2)}$$

ingen Rødder, da $x^2 + x + 1$ for alle hele Værdier af $x$ er et ulige Tal. Som Eksempel paa Kongruenser, der have saa mange Rødder, som Graden angiver, kunne vi nævne

$$x^{p-1} - 1 \equiv 0, \text{ (mod. } p),$$

hvis Rødder ifølge Fermats Sætning ere $1, 2, 3 \ldots p-1$.

For Moduler, der ikke ere Primtal, kan Røddernes Antal baade være mindre end, lig med og større end Kongruensens Grad.

39. Dersom

(17) $$f(x) \equiv \varphi(x)\, \psi(x) \text{ (mod. } p),$$

hvor $\varphi(x)$ og $\psi(x)$ ere Polynomier med hele Koefficienter, deler $f(x) \equiv 0$ sig i de to $\varphi(x) \equiv 0$ og $\psi(x) \equiv 0$.

Sætningens Rigtighed følger af, at et Primtal gaar op i, og kun gaar op i et Produkt, naar det gaar op i den ene Faktor. De to Kongruenser kunne have fælles Rødder og den sammensatte Kongruens faar da lige Rødder.

For sammensatte Moduler gælder Sætningen ikke. Den gælder for Modulus $p^2$, hvis de to Kongruenser ikke mod. $p$ have en fælles Rod, thi da kan $p^2$ kun gaa op i Produktet ved at gaa op i den ene Faktor.

Man maa vel mærke sig, at den omtalte Deling godt kan finde Sted, selv om $f(x) = 0$ ikke er reduktibel i algebraisk Forstand, idet man ved Deling af Kongruensen kan tiltøje hvilke som helst Led, hvis Koefficienter ere delelige med $p$. Som vi saa i 38, er i Virkeligheden enhver Kongruens, der har Rødder for en Primtalsmodulus, reduktibel.

Dersom Kongruensen $f(x) \equiv 0 \pmod{p}$ har saa mange Rødder, som dens Grad angiver og bliver delt i flere andre, maa enhver af disse ogsaa faa saa mange Rødder, som dens Grad angiver, thi hvis en af dem havde færre, maatte en anden af dem have flere, hvilket vi vide er umuligt.

40. Man kan søge de fælles Rødder for to Kongruenser paa samme Maade som for to Ligninger, thi af Ligningen

$$f(x) = \varphi(x)\, Q + R$$

følger, at et Tal, som for en vis Værdi af $x$ gaar op i $f(x)$ og $\varphi(x)$, ogsaa gaar op i $R$, og at det gaar op i $f(x)$, hvis det gaar op i $\varphi(x)$ og $R$. Er den fælles Modulus et Primtal, kan man, som ovenfor vist, altid sørge for, at den første Koefficient i Polynomierne er 1. Hvis vi forudsætte, at $f(x)$ og $\varphi(x)$ ikke have nogen fælles Faktor, faa vi tilsidst en Rest, der er et vist helt Tal $\alpha$, medens den sidst brugte Divisor er f. Eks. $x - \beta$; er $\alpha$ ikke delelig med $p$, have de to Kongruenser ingen fælles Rod; er $\alpha$ delelig med $p$, da er $x \equiv \beta$ fælles Rod.



Har man f. Eks. mod. 5 de to Kongruenser

$$x^2 + 3x + 2 \equiv 0 \text{ og } x^3 + 4x + 1 \equiv 0,$$

da faar man Resten $11x + 7 \equiv x + 2$, der gaar op i den forrige Divisor. 3 er derfor fælles Rod for de to Kongruenser. $x + 2$ er ikke fælles Faktor for de to Polynomier, da man har bortkastet Led, delelige med 5.

41. Enhver Kongruens mod. $p$, som ikke har Nul til Rod, har sine Rødder fælles med Kongruensen

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Vi kunne derfor ved Hjælp af den sidste reducere den givne til en Grad, der er lavere end $p - 1$, og derpaa, ved at søge største fælles Faktor, til en anden, hvis venstre Side er kongruent med en Faktor i $x^{p-1} - 1$, og som derfor har saa mange Rødder som dens Grad angiver.

Vi se saaledes f. Eks. at $x^2 - 5 \equiv 0 \pmod{7}$ ikke har Rødder, thi ved Division af $x^2 - 5$ i $x^6 - 1$ faa vi til Rest 124, der ikke er delelig med 7.

42. Ved Hjælp af 38 faa vi

$$(18)\quad x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\ldots(x-p+1) \pmod{p}$$

og finde deraf ved Sammenligning af Koefficienterne paa de to Sider af Kongruenstegnet, at følgende Udtryk ere delelige med $p$:

$$1 + 2 + 3 + \ldots + p - 1$$
$$1 . 2 + 1 . 3 + \ldots + (p-2)(p-1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$1 . 2 . 3 \ldots (p-1) + 1,$$

saa at vi her blandt andet have et nyt Bevis for Wilsons Sætning.

Om det næstsidste af Udtrykkene ville vi senere vise, at det er deleligt med $p^2$. $(p > 3)$.

43. Vi ville anvende det fundne paa Produktet

$$(kp + 1)(kp + 2) \ldots (kp + p - 1),$$

hvor $k$ er et vilkaarligt helt Tal, ikke deleligt med $p$. Udfører vi Multiplikationen faa vi et Udtryk af Formen

$$Ap^2 + Bkp + 1 . 2 . 3 \ldots (p-1),$$

hvor $B$ er Summen af Produkterne af $p-2$ af Tallene $1, 2, 3 \ldots p-1$ og derfor en af de Summer, som vi fandt var delelig med $p$. Heraf følger da

$$(kp + 1)(kp + 2) \ldots (kp + p - 1) \equiv 1 . 2 . 3 \ldots (p-1) \quad (\text{mod. } p^2),$$

der forøvrigt ogsaa gælder, naar $p$ gaar op i $k$, saa at $B = 0$. Af de to Produkter gaar som bekendt det sidste op i det første, og man har derfor for alle hele Værdier af $k$

(19) $$\frac{(kp + 1)(kp + 2) \ldots (kp + p - 1)}{1 . 2 . 3 \ldots (p-1)} \equiv 1 \ (\text{mod. } p^2).$$

## Den binome Kongruens.

44. Den binome Kongruens $Ax^n \equiv B$ (mod. $k$) ville vi behandle for en vilkaarlig Modulus $k$, som vi dog



tænke os pr. med $A$; vi kunne da ved Multiplikation med et passende Tal bringe den paa Formen

(20) $$x^n \equiv b \ (\text{mod. } k),$$

hvor vi tænke os $b$ pr. med $k$, og hvor da ogsaa de mulige Rødder maa være pr. med $k$. Særlig ville vi betragte Tilfældet $b = 1$, altsaa Kongruensen

(21) $$x^n - 1 \equiv 0. \ (\text{mod. } k).$$

45. Lad $a$ være et vilkaarligt Tal pr. med $k$; vi betragte Rækken af Tal

(22) $$1, a, a^2, a^3, \ldots$$

og deres Rester med $k$. Disse kunne ikke alle være forskellige; lad da $a^r$ og $a^{r+s}$ give samme Rest, medens intet af de mellemliggende Led giver denne Rest; man har da

$$a^r (a^s - 1) \equiv 0. \ (\text{mod. } k),$$

saa at $k$, der er pr. med $a^r$, gaar op i $a^s - 1$. Heraf følger, at et vilkaarligt Led $a^q$ maa give samme Rest som $a^{q+s}$, og at denne Rest ikke kan findes for et mellemliggende Led, da dette vilde medføre, at der mellem $a^r$ og $a^{r+s}$ laa et Led, der gav samme Rest som disse to. Vi slutte heraf, at alle Resterne danne en periodisk Række med $s$ Led i Perioden. Resten 1 findes saaledes for Leddene $1, a^s, a^{2s}, \ldots$ og ikke for andre Led. Man siger, at $a$ **hører til Eksponenten** $s$ **for Modulus** $k$; og udtrykker derved, at $s$ er den laveste Eksponent $(> 0)$, for hvilken $k$ gaar op i $a^s - 1$. Er særlig $s = \varphi(k)$, kaldes $a$ en **primitiv Rod***) for Tallet $k$. Hører $a$ til Eksponenten $s$, maa $s$ være Di-

*) Euler: Comment. nov. Ac. Petrop. T. XVIII. 1773.

visor i $\varphi(k)$, thi $a^{\varphi(k)}$ giver Resten 1, og vi have set, at denne Rest kun findes for Eksponenter, der ere Multipla af $s$. Altsaa:

De $\varphi(k)$ Tal, der ere mindre end og primiske med $k$, maa alle høre til Eksponenter, der ere Divisorer i $\varphi(k)$.

Eks. For $k = 15$ finde vi, at 1 hører til Eksponenten 1; 4, 11 og 14 til 2, 2, 7, 8 og 13 til 4, medens intet Tal hører til Eksponenten $\varphi(15) = 8$. Tallet 15 har saaledes ingen primitive Rødder.

46. Hvis $k$ ikke indeholder Faktorerne 2 og 5, kan man tage $a = 10$; $s$ vil da angive Antallet af Cifre i Perioden, naar man forvandler en Brøk med Nævneren $k$ til Decimalbrøk; er 10 primitiv Rod for $k$, vil Perioden faa $\varphi(k)$ Decimaler og ved Divisionen benyttes alle de $\varphi(k)$ mulige Rester. Til de $\varphi(k)$ ægte, uforkortelige Brøker med Nævneren $k$, maa derfor svare Perioder, der dannes af en af dem ved Cifrenes Kredsforskydning. Det Tal, der danner Perioden for Tælleren 1, har altsaa den Egenskab, at dets Cifre blot kredsforskydes, naar det multipliceres med et vilkaarligt af de Tal, der ere mindre end og pr. med $k$. Det samme gælder naturligvis lige saa godt for ethvert andet Talsystem, naar blot dets Grundtal er primitiv Rod for $k$.

47. Lad $a$ høre til Eksponenten $s$; Rækken af Tal $1, a, a^2, \ldots$ giver da med $k$ kun $s$ forskellige Rester, nemlig de som faas af Tallene

$$1, a, a^2 \ldots a^{s-1},$$

der alle tilfredsstille Kongruensen

$$x^s - 1 \equiv 0. \text{ (mod. } k). \tag{23}$$



Nogle af dem kunne imidlertid høre til lavere Eksponenter, og disse maa da være Divisorer i $s$. Vi kunne bevise, at $a^m$ hører til Eksponenten $\frac{s}{d}$, hvis $d$ er største fælles Maal for $m$ og $s$.

For at bevise dette, søge vi den mindste Værdi af $r$, for hvilken $\frac{mr}{s}$ er et helt Tal; vi forkorte Brøken med største fælles Maal $d$ for $m$ og $s$, og faa derved $\frac{m_1 r}{s_1}$, hvor $m_1$ og $s_1$ ere indbyrdes primiske; for at Brøken skal blive et helt Tal, men da $s_1$ gaa op i $r_1$, saa at den mindst mulige Værdi af $r$ er

$$r = s_1 = \frac{s}{d}.$$

Man har i saa Fald

$$(a^m)^r = (a^s)^{\frac{m}{d}} \equiv 1. \text{ (mod. } k).$$

Vi have saaledes set, at hvis $a$ hører til Eksponenten $s$, saa hører $a^m$ ogsaa til $s$, hvis $m$ er pr. med $s$, og der er saaledes $\varphi(s)$ inkongruente Tal, der hører til denne Eksponent. Men hvis Modulus ikke er et Primtal, er det muligt, at der ikke hører noget Tal til en given Eksponent, og det er muligt, at der hører flere Tal end de angivne til Eksponenten, idet Kongruensen

$$x^s \equiv 1$$

i dette Tilfælde kan have flere end $s$ Rødder. Saaledes for $k = 15$, $s = 4$ kunne vi tage $a = 2$, og deraf følger da, at 8 ogsaa hører til Eksponenten 4, medens 4 hører til Eksponenten 2 og 1 til Eksponenten 1. Men Kongruensen $x^4 \equiv 1$ (mod. 15) har ogsaa Roden 7, der hører til Eksponenten 4, hvad der saa ogsaa gælder om $7^3 \equiv 13$, medens $7^2$ hører til Eksponenten 2, men ikke giver nogen

visor i $\varphi(k)$, thi $a^{\varphi(k)}$ giver Resten 1, og vi have set, at denne Rest kun findes for Eksponenter, der ere Multipla af $s$. Altsaa:

De $\varphi(k)$ Tal, der ere mindre end og primiske med $k$, maa alle høre til Eksponenter, der ere Divisorer i $\varphi(k)$.

Eks. For $k = 15$ finde vi, at 1 hører til Eksponenten 1; 4, 11 og 14 til 2, 2, 7, 8 og 13 til 4, medens intet Tal hører til Eksponenten $\varphi(15) = 8$. Tallet 15 har saaledes ingen primitive Rødder.

46. Hvis $k$ ikke indeholder Faktorerne 2 og 5, kan man tage $a = 10$; $s$ vil da angive Antallet af Cifre i Perioden, naar man forvandler en Brøk med Nævneren $k$ til Decimalbrøk; er 10 primitiv Rod for $k$, vil Perioden faa $\varphi(k)$ Decimaler og ved Divisionen benyttes alle de $\varphi(k)$ mulige Rester. Til de $\varphi(k)$ ægte, uforkortelige Brøker med Nævneren $k$, maa derfor svare Perioder, der dannes af en af dem ved Cifrenes Kredsforskydning. Det Tal, der danner Perioden for Tælleren 1, har altsaa den Egenskab, at dets Cifre blot kredsforskydes, naar det multipliceres med et vilkaarligt af de Tal, der ere mindre end og pr. med $k$. Det samme gælder naturligvis lige saa godt for ethvert andet Talsystem, naar blot dets Grundtal er primitiv Rod for $k$.

47. Lad $a$ høre til Eksponenten $s$; Rækken af Tal $1, a, a^2, \ldots$ giver da med $k$ kun $s$ forskellige Rester, nemlig de som faas af Tallene

$$1, a, a^2 \ldots a^{s-1},$$

der alle tilfredsstille Kongruensen

$$x^s - 1 \equiv 0. \text{ (mod. } k). \tag{23}$$



Nogle af dem kunne imidlertid høre til lavere Eksponenter, og disse maa da være Divisorer i $s$. Vi kunne bevise, at $a^m$ hører til Eksponenten $\frac{s}{d}$, hvis $d$ er største fælles Maal for $m$ og $s$.

For at bevise dette, søge vi den mindste Værdi af $r$, for hvilken $\frac{mr}{s}$ er et helt Tal; vi forkorte Brøken med største fælles Maal $d$ for $m$ og $s$, og faa derved $\frac{m_1 r}{s_1}$, hvor $m_1$ og $s_1$ ere indbyrdes primiske; for at Brøken skal blive et helt Tal, men da $s_1$ gaa op i $r_1$, saa at den mindst mulige Værdi af $r$ er

$$r = s_1 = \frac{s}{d}.$$

Man har i saa Fald

$$(a^m)^r = (a^s)^{\frac{m}{d}} \equiv 1. \text{ (mod. } k).$$

Vi have saaledes set, at hvis $a$ hører til Eksponenten $s$, saa hører $a^m$ ogsaa til $s$, hvis $m$ er pr. med $s$, og der er saaledes $\varphi(s)$ inkongruente Tal, der hører til denne Eksponent. Men hvis Modulus ikke er et Primtal, er det muligt, at der ikke hører noget Tal til en given Eksponent, og det er muligt, at der hører flere Tal end de angivne til Eksponenten, idet Kongruensen

$$x^s \equiv 1$$

i dette Tilfælde kan have flere end $s$ Rødder. Saaledes for $k = 15$, $s = 4$ kunne vi tage $a = 2$, og deraf følger da, at 8 ogsaa hører til Eksponenten 4, medens 4 hører til Eksponenten 2 og 1 til Eksponenten 1. Men Kongruensen $x^4 \equiv 1$ (mod. 15) har ogsaa Roden 7, der hører til Eksponenten 4, hvad der saa ogsaa gælder om $7^3 \equiv 13$, medens $7^2$ hører til Eksponenten 2, men ikke giver nogen

ny Værdi. Saadanne ere imidlertid 11 og 14. Vi have nu ikke andre Tal tilbage, der ere mindre end og pr. med 15, og der hører derfor intet Tal til Eksponenten $8 = \varphi(15)$.

48. Er Modulus et Primtal, saa vide vi, at Kongruensen

$$x^s - 1 \equiv 0 \pmod{p},$$

hvor $s$ er Divisor i $\varphi(p) = p - 1$, højst kan have $s$ Rødder; her gælder da for de forskellige Eksponenter $s$, at der til en saadan enten hører $\varphi(s)$ Tal eller intet; det sidste Tilfælde kan imidlertid ikke indtræffe, thi ethvert Tal maa høre til en af Divisorerne i $p - 1$, saa at man maa have

$$\Sigma \varepsilon \varphi(d) = p - 1,$$

hvor $\varepsilon$ enten er 0 eller 1; men hvis noget $\varepsilon$ var 0, vilde det stride mod 13. Altsaa:

Naar Modulus er et Primtal $p$, vil der til enhver Divisor $s$ i $p - 1$ netop høre $\varphi(s)$ Tal; specielt vil til $p - 1$ høre $\varphi(p-1)$ Tal, saa at et Primtal $p$ har $\varphi(p-1)$ primitive Rødder.

49. Hvis, for en hvilken som helst Modulus, $\alpha$ hører til Eksponenten $a$ og $\beta$ til Eksponenten $b$, og $a$ og $b$ ere indbyrdes primiske, da høre $\alpha\beta$ til Eksponenten $ab$.

I modsat Fald maatte nemlig, da

$$(\alpha\beta)^{ab} \equiv 1,$$

$\alpha\beta$ høre til en Eksponent $\frac{a}{\mu} \cdot \frac{b}{\nu}$, hvor i alt Fald en af Nævnerne f. Eks. $\nu$ ikke er 1; man havde da

$$1 \equiv (\alpha\beta)^{\frac{a}{\mu} \cdot \frac{b}{\nu}} \equiv ((\alpha\beta)^a)^{\frac{a}{\mu} \cdot \frac{b}{\nu}} \equiv \beta^{\frac{a^2}{\mu} \cdot \frac{b}{\nu}}.$$



Her er $\frac{a^2}{\mu}$ pr. med $b$, og man kan derfor bestemme $x$ saaledes, at

$$x \cdot \frac{a^2}{\mu} - yb = 1;$$

heraf vilde følge

$$\beta^{\frac{xa^2}{\mu}} \equiv \beta$$

altsaa
$$1 \equiv \left(\beta^{\frac{xa^2}{\mu}}\right)^{\frac{b}{\nu}} \equiv \beta^{\frac{b}{\nu}},$$

stridende mod, at $\beta$ hører til Eksponenten $b$.

Saaledes for $k = 18$, $\varphi(k) = 6$ hører 17 til Eksponenten 2, 7 til Eksponenten 3, altsaa $7 \cdot 17 \equiv 11$ til Eksponenten $6 \cdot 11$ er altsaa primitiv Rod til 18. 1, 11, $11^2$, $11^3$, $11^4$, $11^5$ ere Rødder i $x^6 \equiv 1$; af dem ere 11 og $11^5 \equiv 5$ primitive, medens $11^2 \equiv 13$ og $11^4 \equiv 7$ høre til Eksponenten 3, og $11^3 \equiv 17$ til Eksponenten 2.

## Primitive Rødder.

50. Vi have set, at alle Primtal have primitive Rødder, og vi have fundet, at 18 har primitive Rødder, men 15 ikke, og vi ville derfor nu stille os den Opgave, at bestemme alle Tal med primitive Rødder.

Lad $a$ være primitiv Rod til Tallet $n$; Tallene

$$a, a^2, a^3 \ldots a^{\varphi(n)}$$

ere da kongruente mod. $n$ med alle Tal mindre end og pr. med $n$; disses Produkt er da kongruent med

$$a^{1+2+3+\ldots+\varphi(n)} = a^{\frac{1}{2}\varphi(n)(\varphi(n)+1)}.$$

Nu er, naar vi undtage $n = 2$, $\varphi(n)$ altid et lige Tal og

$$a^{\varphi(n)+1} \equiv a \pmod{n},$$

saa at det omtalte Produkt

(24) $$1 \cdot a_1 \cdot a_2 \ldots \equiv a^{\frac{1}{2}\varphi(n)},$$

der ikke kan være kongruent med $+1$, da $a$ er primitiv Rod, og derfor maa være kongruent med $-1$; ifølge den udvidede Wilsonske Sætning er imidlertid Betingelsen for, at Produktet af Tallene er kongruent med $-1 \pmod{n}$ den, at Kongruensen

$$x^2 - 1 \equiv 0 \pmod{n}$$

har et ulige Antal Rodpar. For at afgøre, naar dette finder Sted maa vi imidlertid bevise følgende interessante og formentlig ny Sætning:

51. Hvis man dividerer alle de Tal, der ere mindre end og pr. med et Tal $kd$, med en af Tallets Divisorer $d$, da blive Resterne de Tal, der ere mindre end og pr. med $d$, og alle disse Rester forekomme lige mange Gange.

Lad $a_1, a_2, a_3, \ldots$ være de Tal, der ere mindre end og pr. med $kd$ og $\alpha_1, \alpha_2, \alpha_3 \ldots$ være Tallene mindre end og pr. med $d$; vi danne alle Tallene

$$\alpha + qd,$$

hvor $\alpha$ har alle Værdierne $\alpha_1, \alpha_2 \ldots$ og $q$ Værdierne 1, 2, 3, $\ldots k-1$.

Mellem disse Tal findes alle Tallene $a$, da et saadant ved Division med $d$ giver en ufuldstændig Kvotient, som højst er $k-1$ og en Rest, som er pr. med $d$, og derfor er et af Tallene $\alpha$. Hvis vi kun ville have Tallene $a$, maa vi af de Tal, vi have dannet, udskyde alle saadanne, som ikke ere pr. med $k$ og derfor heller ikke med $kd$.

Vi kunne nu udtrykke vor Sætning saaledes:

Antallet af uforkortelige Brøker i Rækken

$$\frac{\alpha}{k}, \frac{\alpha + d}{k}, \frac{\alpha + 2d}{k}, \ldots \frac{\alpha + (k-1)\,d}{k} \tag{25}$$



er det samme, hvilken af Værdierne $\alpha_1, \alpha_2, \alpha_3 \ldots$ vi end indsætte for $\alpha$.

Her er altsaa $k$ og $d$ vilkaarlige hele Tal, medens $\alpha$ betegner alle Tal, mindre end og pr. med $d$.

En fælles Faktor for $k$ og $d$ kan ikke findes i $\alpha$ og saaledes ikke tjene til Forkortning af nogen af Brøkerne; vi ville derfor forudsætte, at $k$ og $d$ ere indbyrdes primiske.

Lad $p_1$ være en Primfaktor i $k$; for at den skal kunne gaa op i en Tæller, maa man have

$$\alpha + xd = yp_1,$$

hvor $y$ er et helt Tal. Da $d$ og $p_1$ ere indbyrdes pr., bestemmer Ligningen een Værdi af $x$, mindre end $p_1$. Lad den tilsvarende Værdi af $y$ være $y_1$. Den fuldstændige Løsning er da

$$x = x_1 + mp_1\,;\, y = y_1 + md, \tag{26}$$

hvor $m$ er et helt Tal, som har Værdievne 0, 1, 2, 3, $k_1 - 1$, idet $k = p_1 k_1$.

Der er saaledes $k_1$ af Tællerne, der ere delelige med $p_1$, altsaa af Tællere, der ikke ere delelige med $p_1$

$$k\left(1 - \frac{1}{p_1}\right),$$

altsaa et Antal, der er uafhængigt af den valgte Værdi af $\alpha$.

Vi kunne udtrykke Resultatet saaledes:

I en Differensrække med $k$ Led, hvor Differensen er primisk med $k$ og med første Led, og hvor $p_1$ er en Primfaktor i $k$, er der

$$k\left(1 - \frac{1}{p_1}\right)$$

Led, som ikke ere delelige med $p_1$.

Er $p_2$ en anden Primfaktor i $k$, faa vi paa samme Maade de Tællere, som ere delelige med $p_2$, udtrykte ved

$$\alpha + (x_2 + mp_2)\, d = \alpha + x_2 d + mp_2 d$$

i Antal $\frac{k}{p_2}$; af disse ere imidlertid nogle delelige med $p_1$; bortdividere vi $p$, faa vi Leddene

$$\frac{\alpha + x_2 d}{p_2} + md \left(m = 0,\ 1, \ldots \frac{k}{p_2}\right),$$

men af disse er der ifølge Sætningen ovenfor $\frac{k}{p_1 p_2}$, der ere delelige med $p_1$, altsaa $\frac{k}{p_2}\left(1 - \frac{1}{p_1}\right)$, der ere delelige med $p_2$, men ikke med $p_1$. Trækkes dette Tal fra det ovenfor fundne, finde vi, at der er

$$k\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

af Tællerne, der ikke ere delelige med $p_1$ eller $p_2$. Fortsætte vi paa samme Maade, finde vi da:

Naar $k$ er primisk med $d$, er der i Rækken af Brøker (25) netop $\varphi(k)$ uforkortelige, uafhængigt af den benyttede Værdi af $\alpha$.

Dette Resultat stemmer med Sætningen i 11; der er $\varphi(kd)$ Tal, som ere mindre end og pr. med $kd$ og $\varphi(d)$, der ere mindre end og pr. med $d$. Naar nu hver af disse forekommer som Rest lige mange Gange, bliver Antallet af Gange $\varphi(kd) : \varphi(d)$, men dette Antal er netop $\varphi(k)$, naar $k$ og $d$ ere indbyrdes primiske (11).

Beviset gælder ogsaa, naar $k$ og $d$ have fælles Divisorer, men Kvotienten er da ikke $\varphi(k)$.

52. Vi vende nu tilbage til den udvidede Wilsonske Sætning; vi antage, at Modulus $n$ har en ulige Primfaktor $p$, og sætte $n = kp$. Vi have da, ifølge den netop beviste Sætning, at de Tal $a_1, a_2, a_3 \ldots$, der ere mindre end og pr. med $kp$, ved Division med $p$ give Resterne $1, 2, \ldots p-1$ lige mange Gange, nemlig $t = \varphi(kp) : \varphi(p)$ Gange. Heraf følger



$$P = a_1\, a_2\, a_3 \ldots \equiv (1.\,2.\,3 \ldots (p-1)^t \equiv (-1)^t \pmod{p}$$

altsaa, at $p$ gaar op i

$$a_1\, a_2\, a_3 \ldots \pm 1,$$

øverste Fortegn, hvis $t$ er et ulige, nederste, hvis $t$ er et lige Tal. Da vi nu har bevist, at $n$ gaar op i et af de to Tal, og $p$ gaar op, naar $n$ gaar op, bliver Produktet $P$ (mod. $n$) kongruent med $+1$ eller $-1$, eftersom $t$ er lige eller ulige. Hvis nu $k$ indeholder en anden ulige Primfaktor end $p$, har man, idet $p_1$ er en saadan Faktor

$$t = \varphi(kp) : \varphi(p) = kp\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p_1}\right) \ldots : \left(p\left(1 - \frac{1}{p}\right)\right)$$

$$= k\left(1 - \frac{1}{p_1}\right) \ldots,$$

der er et lige Tal. Hvis $k$ indeholder Faktoren $2^\alpha$, faar man ogsaa $t$ lige, hvis $\alpha > 1$. Hvis endelig $n$ ikke indeholder nogen ulige Primfaktor, altsaa er af Formen $2^\alpha$, ere Størrelserne $a$ de $2^{\alpha-1}$ laveste ulige Tal; disse ere afvekslende af Formen $4m + 1$ og $4m + 3$, og idet vi tager dem sammen to og to, nemlig 1.3, 5.7 . . ., faa vi $2^{\alpha-2}$ Tal af Formen $4m + 3$, hvis Produkt er af Formen $4m + 1$, undtagen for $\alpha = 2$, $n = 4$. Vi faa saaledes $P \equiv +1$ undtagen for $n = 4$, hvor $P \equiv -1$, hvad der ogsaa gælder for $n = 2$.

I 50 viste vi, at $P \equiv -1$ (mod. $n$) er nødvendig Be-

tingelse for, at $n$ har primitive Rødder; vi have saaledes bevist, at

Der gives ingen andre Tal med primitive Rødder end Potenser af ulige Primtal, det dobbelte af saadanne Tal samt Tallene 2 og 4.

53. Vi have ogsaa udtrykt Betingelsen for, at $n$ har primitive Rødder ved, at

$$x^2 - 1 \equiv 0 \pmod{n} \tag{27}$$

skal have et ulige Antal Rodpar, og ville vise, at dette finder Sted for de fundne Tal. For 2 og 4 ere Rødderne $+1$ og $-1$; for $n = p^\alpha$, maa dette Tal gaa op i $x+1$ eller $x-1$, da disse kun kunne have 2 til fælles Faktor; ogsaa i dette Tilfælde er Rødderne altsaa $+1$ og $-1$. For $n = 2p^\alpha$, maa $x$ være ulige; sætte vi da $x = 2y+1$, maa $p^\alpha$ gaa op i $y$ eller i $y+1$, saa at de eneste Løsninger ere $y = 0$ og $y = -1$, svarende til $x = +1$ og $x = -1$. Kongruensen (27) har saaledes i alle de nævnte Tilfælde kun et Par Rødder.

54. De benyttede Betingelser ere nødvendige, men der kræves Bevis for, at de ogsaa ere tilstrækkelige; vi ville føre dette Bevis saaledes, at vi derved tillige vise, hvorledes de primitive Rødder findes. Vi behøve ikke at opholde os ved Tallene 2 og 4, og for et Primtal $p$ have vi bevist, at der er $\varphi(p-1)$ primitive Rødder, som alle let findes, naar vi kende een af dem.

Lad nu $a$ være primitiv Rod for $p$. I Følge den udvidede Fermatske Sætning gaar $p^\alpha$ op i

$$a^{p^{\alpha-1}(p-1)} - 1.$$



En Divisor i Eksponenten kunne vi skrive som $p^\beta f$, hvor $\beta \leqq \alpha - 1$ og $f$ er en Divisor i $p-1$, hvor dog ikke samtidig $\beta = \alpha - 1$ og $f = p - 1$. Hvis nu $a$ ikke er primitiv Rod for $p^\alpha$, maa man have

$$a^{p^\beta f} \equiv 1 \pmod{p^\alpha}.$$

for visse Værdier af $\beta$ og $f$. Nu er imidlertid

$$a^{p^\beta} \equiv a \,.\, a^{p^\beta - 1} = a \,.\, a^{(p-1)(p^{\beta-1} + p^{\beta-2} + \ldots 1)} \equiv a \pmod{p}$$

saa at $p$ maa gaa op i $a^f - 1$, hvilket, da $a$ er primitiv Rod for $p$, medfører $f = p - 1$. Vi ville nu bevise følgende Sætning:

Hvis $p^m$ er den højeste Potens af $p$, der gaar op i $a^{p-1} - 1$, saa er $p^{m+r}$ den højeste Potens, der gaar op i $a^{p^r(p-1)} - 1$.

Vi forudsætte altsaa, at

$$a^{p-1} = 1 + kp^m,$$

hvor $k$ ikke er delelig med $p$. Ved at opløfte til $p^r$de Potens, faa vi

$$a^{p^r(p-1)} - 1 = p^r \,.\, k \,.\, p^m + \ldots,$$

hvor de udeladte Led ere delelige med højere Potenser af $p$ end den $(m+r)$te, saa at Tallet paa venstre Side er deleligt med $p^{m+r}$, men ikke med en højere Potens af $p$. Af denne Sætning følger nu, at hvis $p^\alpha$ gaar op i

$$a^{p^\beta(p-1)} - 1,$$

saa maa, da $\beta$ højst er lig $\alpha - 2$, $p^2$ eller en højere Potens af $p$ gaa op i $a^{p-1} - 1$; altsaa:

Hvis $p^2$ gaar op i $a^{p-1}-1$, saa er $a$, der er primitiv Rod for $p$, ikke primitiv Rod for $p^\alpha$, hvor $\alpha > 1$.

I dette Tilfælde, hvor $a$ ikke er primitiv Rod, kan man imidlertid benytte $a$ til at finde primitive Rødder, idet vi kunne bevise, at

Naar $a$ er primitiv Rod for $p$, men ikke for $p^\alpha$, ville alle Tallene $a + bp$, hvor $b$ betegner ethvert af de Tal, der ere mindre end $p^\alpha$, og ikke delelige med $p$, være primitive Rødder for $p^\alpha$.

Vi have nemlig

$$(a + bp)^{p-1} - 1 = a^{p-1} - 1 + (p-1)\, a^{p-2} bp + \text{Multiplum af } p^2$$

som, da $a^{p-1}$ er delelig med $p^2$, viser, at venstre Side ikke er delelig med $p^2$, saa at $a + bp$, der er primitiv Rod for $p$, ogsaa er primitiv Rod for $p^\alpha$. Vi have saaledes af $a$ udledt $\varphi(p^\alpha)$ primitive Rødder for $p^\alpha$.

Hvis $a^{p-1}-1$ ikke er delelig med $p^2$, er der et af Tallene $a + bp$, for hvilket Differensen er delelig med $p^2$, saa at Tallet ikke er primitiv Rod for $p^\alpha$; vi finde dette, naar vi bestemme $b$ af Kongruensen

$$\frac{a^{p-1}-1}{p} + (p-1)\, a^{p-2} b \equiv 0 \pmod{p}$$

der, da $p$ ikke gaar op i første Led eller i Koefficienten til $b$, har een Løsning. Idet vi nu sætte den saaledes bestemte Værdi af $a + bp$ i Stedet for $a$, gælder Udviklingen ovenfor, og vi have saaledes:

Naar vi af en vilkaarlig primitiv Rod $a$ for $p$ danner Rækker af $\varphi(p^\alpha) + 1$ Tal $a + bp$, hvor $b$ betyder alle Tal mindre end og primiske med $p^\alpha$ samt 0, er der i hver saadan Række et og kun et Tal, der ikke er primitiv Rod for $p^\alpha$.



Det hele Antal af primitive Rødder for $p^\alpha$ er saaledes:

$$(28) \qquad \varphi(p-1)\, \varphi(p^\alpha) = \varphi(p^\alpha (p-1))$$

55. Vi gaa nu over til Undersøgelse af Tallene $2p^\alpha$ Lad $a$ være et ulige Tal, som hører til Eksponenten $m$ for Modulus $p^\alpha$ og til Eksponenten $n$ for Modulus $2p^\alpha$, altsaa

$$a^m - 1 \equiv 0 \pmod{p^\alpha} \text{ og } a^n - 1 \equiv 0 \pmod{2p^\alpha}$$

Nu er imidlertid den første Differens et lige Tal, saa at man ogsaa har

$$a^n - 1 \equiv 0 \pmod{2p^\alpha}.$$

hvoraf følger, at $m$ gaar op i $n$; da man ogsaa har

$$a^n - 1 \equiv 0 \pmod{p^\alpha},$$

maa ogsaa $n$ gaa op i $m$. De to Eksponenter ere altsaa lige store. Da nu $\varphi(p^\alpha) = \varphi(2p^\alpha)$ følger heraf, at hvis $a$ er primitiv Rod for det ene af Tallene, er det ogsaa primitiv Rod for det andet. Vi maa imidlertid erindre, at vi have forudsat, at $a$ er et ulige Tal. Nu er alle de Tal, der ere primiske med $2p^\alpha$, ulige, men for $p^\alpha$ kan der være lige primitive Rødder mindre end $p^\alpha$. Erstatte vi imidlertid en saadan Rod $a$ ved $a + p^\alpha$, faa vi en ulige Rod. Vi have saaledes:

Til Tallene $p^\alpha$ og $2p^\alpha$ høre de samme primitive Rødder, naar vi tage de til $p^\alpha$ hørende som ulige Tal.

56. Vi have saaledes fundet Antallet af primitive Rødder, og vist, hvorledes de kunne findes; her er dog et Undtagelsestilfælde; vi have vist, at et Primtal $p$ har $\varphi(p-1)$ primitive Rødder, og at disse alle kunne findes, naar vi kende een af dem; men til at finde een har man ingen anden Metode end Forsøg. Vil man prøve, om $a$ er primitiv Rod for $p$, danner man Rækken $a, a^2 \ldots$, idet man dog stadig dividerer med $p$ og kun beholder Resten. Saaledes for $p = 19$, $a = 2$ faar man

$$2,\ 4,\ 8,\ 16,\ 13,\ 7,\ 14,\ 9,\ -1.$$

Længere behøver man ikke at fortsætte, da 9 er den største Divisor i 18 med Undtagelse af 18 selv.

Her følger de laveste primitive Rødder for Primtallene lavere end 100:*)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
| 2 | 2 | 3 | 2 | 2 | 3 | 2 | 5 | 2 | 3 | 2 | 6 | 3 |
| 47 | 53 | 59 | 61 | 67 | 71 | 73 | 79 | 83 | 89 | 97 | | |
| 5 | 2 | 2 | 2 | 2 | 7 | 5 | 3 | 2 | 3 | 5 | | |

Nogen Lettelse kan maaske faas ved Anvendelse af Sætningen 49, idet man opløser $p-1$ i indbyrdes pr. Faktorer og søger de Tal, der høre til disse som Eksponenter; saaledes for $p = 41$, faar man

$$x^5 - 1 \equiv 0 \pmod{41} \text{ og } x^8 - 1 \equiv 0 \pmod{41},$$

hvor de til Eksponenterne 5 og 8 hørende Tal bestemmes ved

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \text{ og } x^4 + 1 \equiv 0,$$

der henholdsvis give $x = 10$ og $x = 3$, altsaa 30 som primitiv Rod for 41. Nu er $30^7 \equiv 6$, som er den ovenfor angivne primitive Rod.

*) Crelles Journal Bd. 9.



**Basis og Index. Rester og Ikkerester.**

57. Da alle Tallene $1, 2, 3 \ldots p-1$ ere kongruente med forskellige Potenser af en til $p$ hørende primitiv Rod, kan dette benyttes til Indførelse af en Slags Logaritmeregning. Er $g$ den primitive Rod og

$$g^m \equiv a \pmod{p}, \tag{29}$$

kaldes $m$ Index til $a$ for Basis $g$. Af Formlen følger, at man kan regne med Indices som med Logaritmer, idet man dog maa erindre, at Index kun er bestemt paa et Multiplum af $p-1$ nær, da $g^{p-1} \equiv 1$. Medens Tallet er at tage efter Modulus $p$, bliver saaledes Index at tage efter Modulus $p-1$. Som Eksempel følger her en Indextavle for $p = 19$; $g = 2$.*)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| *Tal* | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| *Index* | 0 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 |
| *Tal* | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 + Multip. af 19 | | |
| *Index* | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 + Multip. af 18 | | |

Af Definitionen følger straks, at man for enhver Basis har

$$\text{Ind. } 1 = 0;\ \text{Ind. } (-1) = \tfrac{1}{2}(p-1). \tag{30}$$

Har man dannet sig en Indextabel for et Primtal $p$, kan man ved Hjælp af den løse forskellige Kongruenser med Modulus $p$. Saaledes af Kongruensen af første Grad

$$ax \equiv b \pmod{p},$$

faar man

$$\text{Ind. } x = \text{Ind. } b - \text{Ind. } a.$$

Saaledes af

$$13\,x \equiv 5 \pmod{19}$$

*) I Canon Arithmeticus af Jacobi (1839) findes Indextabeller for Primtallene mindre end 1000.

faar man

$$\text{Ind. } x = \text{Ind. } 5 - \text{Ind. } 13 = 16 - 5 = 11\,;\ x = 15 + 19\,m.$$

Af

$$x^n \equiv a \ (\text{mod. } p) \tag{31}$$

følger

$$\text{Ind. } x = \frac{\text{Ind. } a + m\,(p-1)}{n} = z,$$

hvor $nz \equiv \text{Ind. } a.\ (\text{mod. } p-1)$,

en Kongruens, der, som tidligere vist, har een Løsning, hvis $n$ er pr. med $p-1$. Er derimod $f$ største fælles Maal for $n$ og $p-1$, har $z$ $f$ Værdier, dersom $f$ gaar op i Ind. $a$, medens der ingen Løsninger findes, dersom $f$ ikke gaar op i Ind. $a$. Man maa derfor, for at der skal være Løsninger, have

$$n = fn_1\,;\ p-1 = fr\,,\ a = g^{fm},$$

hvor $n_1$ og $r$ ere indbyrdes primiske; man faar da

$$n_1 \text{ Ind. } x \equiv m \left(\text{mod. } \frac{p-1}{f}\right),$$

der bestemmer een Værdi, mindre end $r$ for Ind. $x$. Er denne Værdi $\alpha$, bliver den almindelige Løsning

$$\alpha + k\,.\,\frac{p-1}{f}\,.\,(k = 0,\ 1, 2\ \ldots f-1),$$

Saaledes for

$$x^{15} \equiv 7\,.\ (\text{mod. } 19)$$

faa vi, idet Ind. $7 = 6$, $f = 3$,

$$5 \text{ Ind. } x \equiv 2 \ (\text{mod. } 6)$$

$$\text{Ind. } x = 4,\ 10,\ 16\,;\ x = 16,\ 17,\ 5.$$

Vi kunne udlede Mulighedsbetingelsen paa en anden Maade, der viser dens Uafhængighed af den valgte Basis. Af

$$a = g^{fm}$$



faa vi

$$a^{\frac{p-1}{f}} \equiv 1 \ (\text{mod. } p),$$

og af denne Kongruens kan atter den første udledes; er nemlig $a \equiv g^z$ faar man

$$g^{z\,.\,\frac{p-1}{f}} \equiv 1\,.\ (\text{mod. } p)$$

der, da $g$ er primitiv Rod, viser, at $f$ maa gaa op i $z$. Vi have saaledes:

*Den nødvendige og tilstrækkelige Betingelse for, at Kongruensen*

$$x^n \equiv a \ (\text{mod. } p)$$

*har Løsninger er, at*

$$a^{\frac{p-1}{f}} \equiv 1 \ (\text{mod. } p), \tag{32}$$

*hvor $f$ er største fælles Maal for $n$ og $p-1$.*

De Tal $a$, for hvilke der er Løsninger, kaldes de $n$*te Potensrester* for $p$; de andre Tal *Ikkerester*. For $n = 2$, 3, 4 kaldes Resterne henholdsvis *kvadratiske, kubiske* og *bikvadratiske*.

58. Af Kongruensen

$$x^2 \equiv -1\,.\ (\text{mod. } p),$$

hvor $p$ er et ulige Primtal, faa vi, idet vi her have $f = 2$

$$\text{Ind. } x = \frac{p-1}{4} + k\,\frac{p-1}{2}, \qquad (k = 0,\ 1)$$

der viser, at Opgaven er uden Løsning, hvis $p$ er af Formen $4n-1$, medens den har to Løsninger for $p = 4n+1$. Altsaa:

Tallet $-1$ er kvadratisk Rest for Primtal af Formen $4n+1$, men Ikkerest for Primtal af Formen $4n+3$

eller

Et Tal af Formen $x^2+1$ er ikke deleligt med nogen Primfaktor af Formen $4n-1$, medens det er deleligt med et vilkaarligt Primtal af Formen $4n+1$ for to Værdier af $x$, mindre end Primtallet.

Af Kongruensen

$$x^{32} \equiv -1 \pmod{p}$$

faar man

$$\text{Ind. } x = \frac{p-1}{64} + k\,\frac{p-1}{f},$$

hvor det sidste Led er et helt Tal; man ser heraf, at Tallet $x^{32}+1$ kun kan indeholde Primfaktorer af Formen $64n+1$. Tallet $2^{32}+1$, der spiller en Rolle ved Cirkelperiferiens Deling, blev anset for et Primtal, indtil *Euler* fandt, at det er deleligt med 641. Efter hvad vi have vist, har Euler kun behøvet at prøve med Primtallene 193, 257, 449, 577, 641 for at opløse Tallet i Faktorer, og af disse kræver $257 = 2^8+1$ ingen Regning.

59. Hvis Modulus ikke er et Primtal, men hører til de Tal, der have primitive Rødder, kan man ogsaa danne en Indextabel, men da vi her kun ville betragte den binome Kongruens af anden Grad, men for en vilkaarlig Modulus, ville vi gaa en anden Vej.

Vi antage da, at vi have

(33) $$x^2 \equiv a \pmod{n},$$

hvor vi først ville tænke os $n$ ulige og $a$ pr. med $n$. Vi



ville antage, at $x = x_1$ er en Løsning og sætte $x = x_1 z$, hvorved

$$x_1^2\,(z^2-1) \equiv 0 \pmod{n}$$

eller, da $n$ er pr. med $x_1$,

(34) $$z^2 - 1 \equiv 0 \pmod{n},$$

der viser, at vi faa alle Løsninger af (33), naar vi multiplicere en af Løsningerne med alle Løsninger af (34). For at finde disse bemærke vi, at $x+1$ og $x-1$ kun kunne have 2 til fælles Faktor, og at derfor det ulige Tal $n$ for at gaa op i $x^2-1$ maa dele sig i to indbyrdes pr. Faktorer, af hvilke den ene gaar op i $x-1$, den anden i $x+1$. Kalde vi den første $\alpha$, faa vi $x = 1 + y\alpha$; $x+1 = 2 + y\alpha$, hvor $y$ er et helt Tal, og

$$\alpha y \equiv -2 \left(\text{mod. } \frac{n}{\alpha}\right),$$

som, da de to Faktorer $\alpha$ og $\frac{n}{\alpha}$ efter vor Forudsætning ere indbyrdes pr., har een Løsning. Der er derfor saa mange Løsninger, som der er Maader at opløse $n$ paa i to indbyrdes pr. Faktorer. Er nu

$$n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

bliver det søgte Antal lig Antallet af Divisorer i Tallet

$$p_1\, p_2\, p_3 \ldots p_r,$$

et Antal, som vi have fundet i 6 er $2 \cdot 2 \ldots = 2^r$.

Dette Antal forandres ikke, dersom vi føje Faktoren 2 til $n$, thi $x$ maa da være ulige, og vi kunne forudsætte, at Faktoren 2 ved Opløsningen altid skal findes i en bestemt af Faktorerne f. Eks. i $\alpha$.

Er $n = 4m$, og sætte vi $x = 2y + 1$, faa vi

$$y(y+1) \equiv 0 \pmod{m},$$

der, da $y$ og $y + 1$ ere indbyrdes pr., har $2^r$ Løsninger, hvis $m$ indeholder $r$ forskellige Primfaktorer, idet 2 ikke her spiller nogen særlig Rolle. Til hver Værdi af $y$ svarer imidlertid to Værdier af $x$, nemlig $2y + 1$ og $2(y + m) + 1$. Altsaa:

Kongruensen (34) har $2^r$ Løsninger, hvis $n$ ikke er delelig med 4 og indeholder $r$ forskellige ulige Primfaktorer; den har $2^{r+1}$ Løsninger, hvis $n:4$ indeholder $r$ forskellige Primfaktorer.

Vi se heraf, at (34) altid har et lige Antal Rodpar, undtagen naar $n$ er en Potens af et ulige Primtal eller det dobbelte af en saadan Potens eller 2 eller 4 og have derved atter fundet de Tilfælde, i hvilke $n$ har primitive Rødder.

60. Idet vi bibeholde Benævnelsen kvadratisk Rest for et Tal $a$, for hvilket Kongruensen (33) har Løsninger, kunne vi nu bestemme disse Resters Antal. Idet vi for $a$ indsætte en Rest (vi benytte herefter denne Betegnelse, naar det ikke kan medføre Misforstaaelse), faa vi for $x$ saa mange Værdier, mindre end og pr. med $n$ som Kongruensen (34) har Løsninger; da der paa den anden Side til enhver saadan Værdi af $x$ svarer en Værdi af $a$, have vi:

Antallet af kvadratiske Rester for et Tal $n$ er $\varphi(n)$, divideret med Antallet af Løsninger af Kongruensen $x^2 - 1 \equiv 0. \pmod{n}$.



Have vi saaledes $n = pq$, hvor $p$ og $q$ ere ulige Primtal, saa er $\varphi(n) = (p-1)(q-1)$ og Kongruensen (34) har $2^2$ Løsninger. Antallet af Rester for $pq$ er derfor

$$\tfrac{1}{4}(p-1)(q-1).$$

Der hører saaledes til Tallet 21 kun 3 Rester, og da et Kvadrattal altid er en Rest, maa disse være Tallene 1, 4 og 16 (9 er ikke pr. med 21); dette vil altsaa sige, at hvis vi kvadrere de 12 Tal, der ere mindre end og pr. med 21, faa vi kun Tal, der ere kongruente med de 3 Rester.

For et Primtal $p$ faa vi, at der er $\frac{1}{2}(p-1)$ Rester, altsaa lige mange Rester og Ikkerester.

61. Er $p$ et Primtal og $a$ en dertil hørende Rest, har man

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p},$$

saa at alle Resterne tilfredsstille Kongruensen

$$x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}, \tag{35}$$

og da denne Kongruens netop har $\frac{1}{2}(p-1)$ Rødder, maa alle Ikkeresterne tilfredsstille Kongruensen

$$x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}. \tag{36}$$

*Legendre* har herfor indført Symbolerne

$$\left(\frac{x}{p}\right) = +1 \text{ og } \left(\frac{x}{p}\right) = -1,$$

der saaledes henholdsvis betegne at $x$ er Rest eller Ikkerest for Primtallet $p$. Vi ville for Kortheds Skyld, hvor det ikke kan misforstaas, betegne Rester og Ikkerester

henholdsvis ved $R$ og $I$ ($r$ og $i$ med tilføjede Indices), og de to Kongruenser (35) og (36) vise da, at man har

$$RR = R;\ RI = I;\ II = R;$$

altsaa

Produktet af to $R$ eller af to $I$ er en $R$, medens Produktet af en $R$ og en $I$ er en $I$, hvad vi ogsaa kunne udtrykke ved Ligningen

$$(37)\qquad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\ldots = \left(\frac{a\,b\,c\ldots}{p}\right).$$

Ethvert Kvadrattal er en Rest, og vi kunne finde alle $R$ som Divisionsrester ved at dividere $1^2$, $2^2 \ldots \left(\frac{p-1}{2}\right)^2$ med $p$; gaar man videre med Kvadrattallene, faar man atter Resterne, idet

$$n^2 \equiv (p-n)^2 \pmod{p}.$$

62. Hvis et Tal $a$ er en $I$, kan man parre Tallene $1, 2 \ldots p-1$ to og to, saa at to parrede Tals Produkt er kongruent med $a$; er derimod $a$ en $R$, ville to af Tallene falde sammen med deres parrede, og Produktet af disse to Tal er kongruent med $-a$ (smlgn. 36).

Man faar altsaa:

$$1 . 2 . 3 \ldots (p-1) \equiv a^{\frac{p-1}{2}} \pmod{p}\ (a \text{ en } I)$$

$$1 . 2 . 3 \ldots (p-1) \equiv -\,a^{\frac{p-1}{2}} \pmod{p}\ (a \text{ en } R).$$

Heraf følger for $a = 1$ Wilsons Sætning, og derpaa de to Kongruenser (35) og (36), af hvilke atter Fermats Sætning kan udledes ved Multiplikation. Denne Udvikling giver saaledes paa en Gang tre af Talteoriens Hovedsætninger.



63. Vi ville nu gaa frem som ovenfor, men af Tallene mindre end $p$ kun betragte Resterne; vi kunne da ved Løsning af Kongruenser af første Grad parre Resterne to og to, saaledes at Produktet af to parrede er kongruent med en vilkaarlig valgt Rest $a$. Her kan dog det Tilfælde indtræde, at en Rest falder sammen med sin parrede; dette indtræder for Rester, der bestemmes ved Kongruensen

$$(38)\qquad x^2 - a \equiv 0 \pmod{p}.$$

Her kan nu indtræde to Tilfælde:

$\boldsymbol{p = 4n+1.}$ — 1, altsaa ogsaa $-a$ er Rest; følgelig maa de to Værdier af $x$, som bestemmes af (38) være begge $R$ eller begge $I$. Da vi nu kun betragte Resterne, kan i det sidste Tilfælde alle de $2n$ Rester lade sig parre to og to med Produktet $a$; medens i det første Tilfælde de to Rester, der bestemmes ved (38) have Produktet $-a$. I dette Tilfælde er $x$ kongruent med et Kvadrat, altsaa $a$ en bikvadratisk Rest. Vi faa altsaa, naar vi ved $P_r$ forstaa Produktet af Resterne,

$$(39)\qquad P_r \equiv \mp\, a^{\frac{p-1}{4}} \pmod{p},$$

øverste Fortegn, naar $a$ er bikvadratisk Rest, nederste, naar $a$ kun er kvadratisk Rest. Da 1 er bikvadratisk Rest faa vi for $a = 1$

$$P_r \equiv -1 \pmod{p = 4n+1}$$

og derpaa

$$a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$$

med de samme Betingelser.

$\boldsymbol{p = 4n-1.}$ $-1$ og derfor ogsaa $-a$ er $I$, saa at

af de to Værdier af $x$ den ene er $R$, den anden $I$. Lad den første være $\alpha$; vi have da

$$P_r \equiv \alpha \,.\, a^{\frac{p-3}{4}},$$

For $a = 1$ er $\alpha = 1$, og vi faa

(40) $$P_r \equiv 1 \text{ (mod. } p = 4n - 1).$$

Vi have saaledes:

Produktet af Resterne er henholdsvis kongruent med $-1$ eller $+1$, eftersom Primtallet $p$ er af Formen $4n+1$ eller $4n-1$.

Vi kunne forøvrigt ogsaa bevise denne Sætning saaledes:

Er $g$ primitiv Rod, have vi

$$P_r \equiv g^2 . g^4 . g^6 \ldots g^{p-1} = g^{\frac{(p+1)\,(p-1)}{4}} = g^{\frac{p-1}{2} \cdot \frac{p+1}{2}}$$

$$\equiv (-1)^{\frac{p+1}{2}} \equiv \begin{matrix} +1 \; (p = 4n - 1) \\ -1 \; (p = 4n + 1). \end{matrix}$$

For $p = 4n - 1$ fandt vi, at der til enhver Rest $a$ svarer en Rest $\alpha$, der tilfredsstiller Kongruensen (38). Sætte vi nu $\alpha \equiv \beta^2$ (mod. $p$), giver (38) os

altsaa: $$a \equiv \beta^4 \text{ (mod. } p),$$

Alle kvadratiske Rester for $p = 4n - 1$ ere ogsaa bikvadratiske Rester.

Dette stemmer ogsaa med Betingelsen (32)... Største fælles Maal for 4 og $p - 1$ er 2

og $$a^{\frac{p-1}{2}} \equiv 1 \text{ (mod. } p = 4n - 1)$$

bliver derfor Betingelse for, baade at $a$ er kvadratisk og bikvadratisk Rest.

---

# TREDIE KAPITEL

## KVADRATISKE RESTER

### Reciprocitetssætningen.

64. Vi have set, at Betingelsen for, at et Tal $a$ er kvadratisk Rest for et Primtal $p$, er, at

(1) $$a^{\frac{1}{2}(p-1)} \equiv 1 \text{ (mod. } p),$$

en Betingelse, hvis Anvendelse for voksende $p$ hurtigt bliver praktisk talt uigennemførlig. En betydelig Lettelse naaede man ved Legendres Reciprocitetssætning, der fører til en Algoritme, ved hvilken man stadig reducerer Opgaven til den samme Opgave for lavere Tal. Legendre gav intet Bevis for Sætningen, men senere gav Gauss 6 saadanne, der grundedes paa meget forskellige Principer. Metoden naaede imidlertid først sin fulde Betydning ved en Udvidelse af *Jacobi*. Det Bevis, vi her skulle give, slutter sig nærmest til Gauss' tredje Bevis, hvad det har fælles med nogle andre senere fremkomne Beviser, men medens disse kun beviser Sætningen i dens oprindelige Form, gælder Forfatterens for Sætningen i dens største Almindelighed. Det offentliggjordes første Gang i Tidsskrift for Matematik 1879.

Lad $a$ og $b$ være to hvilkesomhelst indbyrdes primiske Tal, $b$ ulige. Tallene

$$a, 3a, 5a \ldots (b-2)\, a$$

divideres med $b$ saaledes, at man faar lutter ulige Rester, liggende mellem $-b$ og $+b$, dette kan altid opnaas ved at tage Kvotienterne lige eller ulige, eftersom $a$ er ulige eller lige og forøvrigt af en passende Størrelse. Resterne maa alle være numerisk forskellige, thi hvis to af dem vare numerisk lige store, maatte $b$ gaa op i Summen eller Differensen af to af de ulige Tal, med hvilke $a$ er multipliceret; dette er imidlertid umuligt, da Differensen er mindre end $b$, og Summen et lige Tal, mindre end $2b$. Resterne maa derfor netop være de ulige Tal, med hvilke vi have multipliceret $a$, kun at nogle af dem ere negative. Ved Tegnene

$$\left(\frac{a}{b}\right) = +1\,;\left(\frac{a}{b}\right) = -1. \tag{2}$$

ville vi nu betegne henholdsvis, at de negative Rester forekomme i lige eller ulige Antal. At Tegnene ere de samme som de Legendreske Symboler kan ikke foraarsage Misforstaaelser, thi de stemme overens i de Tilfælde, hvor Legendres Tegn overhovedet have Betydning, nemlig naar $b$ er et Primtal; man faar nemlig ved Multiplikation

$$1.3.5\ldots(b-2)\,a^{\frac{b-1}{2}} \equiv \pm 1.3.5\ldots(b-2) \pmod{b}$$

eller

$$1.3.5\ldots(b-2)\,(a^{\frac{b-1}{2}} \mp 1) \equiv 0 \pmod{b},$$

der viser, at naar $b$ er et Primtal, svarer de to Betegnelser henholdsvis til, at $a$ er $R$ eller $I$ ligesom hos Legendre. Er $b$ derimod ikke et Primtal, faar Symbolerne ikke noget med $R$ og $I$ at gøre, men angive kun, om Antallet af negative Rester ved Divisionerne er lige eller ulige. Man ser straks, at man i Stedet for $a$ kan sætte ethvert dermed (mod. $b$) kongruent Tal.



Vi sætte nu $a = a_1 a_2$ og behandle $a_1$ som før $a$; vi faa derved

$$1.3.5\ldots(b-2)\,a_1^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) 1.3.5\ldots(b-2) \pmod{b}$$

eller, hvis Ligningerne, før de multipliceres med hinanden, alle først multipliceres med $a_2$

$$1.3.5\ldots(b-2)\,a^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) 1.3.5\ldots(b-2)\,a_2^{\frac{b-1}{2}}$$

hvoraf

$$\left(\frac{a}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right) \tag{3}$$

65. Før vi gaa videre i Udviklingen, ville vi betragte et Par specielle Tilfælde.

Af Ligningen

$$\left(\frac{k^2}{b}\right) = \left(\frac{k}{b}\right)\left(\frac{k}{b}\right) = 1$$

se vi, at vi af Tallet i Tælleren kunne bortdividere et Kvadrat, uden at Symbolets Værdi forandrer Fortegn.

Er $a = -1$, blive alle Resterne negative, og man har saaledes

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \tag{4}$$

Er $a = 2$, faa vi Rækken

$$1.2,\ 3.2,\ 5.2,\ldots(b-2)\,2,$$

der give negative Rester, saa længe Leddene er mindre end $b$. Disses Antal bliver lige, hvis $b$ er en af Formerne $8_n + 1$ og $8_n + 7$, ulige, hvis $b$ er en af Formerne $8_n + 3$, $8_n + 5$. Dette udtrykkes ved Ligningen

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} \tag{5}$$

66. Vi vende nu tilbage til det almindelige Tilfælde, hvor vi dog kunne forudsætte, at $a$ er ulige, da vi ved (5) kunne bortskaffe Faktoren 2. Endvidere kunne vi forudsætte $a < b$. Vi faa da ved Division Ligninger af Formen

(6) $$(2n + 1)\,a - 2mb = r,$$

hvor $2n + 1$ højst er $b - 2$ og $2m$ højst $a - 1$. Den samme Værdi af $2m$ kan findes i flere paa hinanden følgende Ligninger, og de tilsvarende Rester danne da en Differensrække med Differensen $2a$; der maa derfor for enhver Værdi af $2m$ findes netop een Rest, som ligger mellem $-a$ og $+a$. Ligningen kan omskrives til

(7) $$(a - 2m)\,b - (b - 2n - 1)\,a = r.$$

$a - 2m$ har her efterhaanden Værdierne $1, 3, 5 \ldots (a-2)$, og Ligningerne ere saaledes netop de, der bestemme $\left(\frac{b}{a}\right)$; vi gaa imidlertid kun ud paa at bestemme Forholdet mellem $\left(\frac{a}{b}\right)$ og $\left(\frac{b}{a}\right)$ og kunne derfor udelade alle de Rester $r$, der benyttes begge Steder, det vil sige de Rester, der ligge mellem $-a$ og $+a$. Da nu Resterne mellem $+a$ og $+b$ ere positive, behøve vi kun at betragte de Rester, der ligge mellem $-b$ og $-a$; eftersom disses Antal er lige eller ulige, ville de to Symboler have samme eller forskellige Fortegn. Vi sætte altsaa

$$-b < (2n + 1)\,a - 2mb < -a.$$

Vi sætte her $m = n - k$; $a = b - 2\alpha$ og faa da ved nogen Omskrivning

$$2n + 1 < \frac{(k+1)\,b}{\alpha} < 2n + 2.$$



Da den største Værdi af $2n + 1$ er $b - 2$, altsaa $b - 1$ den største Værdi af $2n + 2$, bliver $\alpha - 1$ den største Værdi af $k + 1$, medens $k$ ikke kan være negativ; vi have saaledes Rækken af Brøker

$$\frac{b}{\alpha},\ \frac{2b}{\alpha},\ \frac{3b}{\alpha} \ldots \frac{(\alpha - 1)\,b}{\alpha},$$

og enhver af disse bestemmer en negativ Rest mellem $-b$ og $-a$, dersom dens nærmest lavere hele Tal er ulige. Det gælder altsaa om at finde, om det Antal Brøker, der har denne Egenskab, er lige eller ulige.

Nu er imidlertid Summen af den første og den sidste, af den næstførste og den næstsidste og saaledes videre lig $b$, og da $b$ er et ulige Tal maa to af de saaledes parrede Brøker have deres nærmest lavere hele Tal begge lige eller begge ulige, og kunne derfor udelades.

Hvis nu $\alpha$ er ulige, blive alle Leddene parrede, og det søgte Antal negative Rester er lige. I dette Tilfælde ere af de ulige Tal $a$ og $b$, det ene af Formen $4n + 1$, det andet af Formen $4n + 3$; er $\alpha$ lige, beroer Resultatet paa det mellemste Led, der er $\frac{1}{2}\,b$. $b$ og $a$ ere begge af Formen $4n + 1$ eller $4n + 3$. I det første Tilfælde er det største hele Tal i $\frac{1}{2}\,b$ lige og bestemmer derfor ingen negativ Rest, medens det bestemmer en saadan i det andet Tilfælde, da det største hele Tal i $\frac{1}{2}\,b$ er ulige.

Vi have saaledes bevist, at vi have $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ i alle Tilfælde, undtagen, naar de ulige Tal $a$ og $b$ begge ere af Formen $4n + 3$. Dette kan udtrykkes ved Ligningen

(8) $$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Regningerne blive nu omtrent de samme som ved Bestemmelsen af de to Tals største fælles Maal. Saaledes faa vi f. Eks.

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right) = -\frac{11}{365}$$

$$= -\left(\frac{365}{11}\right) = -\left(\frac{2}{11}\right) = 1,$$

der viser os, at 365 er $R$ for Primtallet 1847.

67. Ved Hjælp af den udvidede Reciprocitetssætning kunne vi saaledes afgøre, om et givet Tal er $R$ eller $I$ for et givet Primtal; hvorledes man kan benytte Sætningen til at finde lineære Former for de Primtal, for hvilke et givet Tal er $R$, skulle vi nu vise, ved at udføre Bestemmelsen for de laveste Tal. Vi have allerede fundet, at $-1$ er $R$ for $p = 4n + 1$, $I$ for $p = 4n - 1$.

For Tallet 2 fandt vi

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

der viser, at 2 er $R$, naar $p^2 - 1$ er delelig med 16; Tal af Formen $8n - \alpha$ kunne kun være Primtal for $\alpha = 1, 3, 5, 7$ og Betingelsen tilfredsstilles for $\alpha = 1$ og 7.

2 er derfor $R$ for $p = 8n + 1$ og $8n + 7$; $I$ for $p = 8n + 3$ og $8n + 5$.

Skal $-2$ være $R$, maa $-1$ og 2 begge være $R$ eller begge $I$. Altsaa

$-2$ er $R$ for $p = 8n + 1$ og $8n + 3$. $I$ for $p = 8n + 5$ og $8n + 7$.

For at undersøge Tallet 3, betragte vi Tallene $12n + \alpha$, hvor $\alpha = 1, 5, 7, 11$; vi have



$$\left(\frac{3}{12n+1}\right) = \left(\frac{1}{3}\right) = 1;\ \left(\frac{3}{12n+5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) =$$

$$-1;\ \left(\frac{3}{12n+7}\right) = -\left(\frac{7}{3}\right) = -1;\ \frac{3}{12n+11} = -\left(\frac{11}{3}\right) = +1,$$

altsaa

3 er $R$ for $p = 12n + 1$ og $12n + 11$, $I$ for $p = 12n + 5$ og $12n + 7$,

og følgelig

$-3$ er $R$ for $p = 12n + 1$ og $12n + 7$, $I$ for $p = 12n + 5$ og $12n + 11$ eller $R$ for $6n + 1$, $I$ for $6n - 1$.

For at undersøge 5 betragte vi Tallene $10n + \alpha$; $\alpha = 1, 3, 7, 9$ og faa $\left(\frac{5}{10n+\alpha}\right) = \left(\frac{\alpha}{5}\right)$, der for $\alpha = 1$ og 4 giver $+1$, for $\alpha = 2$ og 3 giver $-1$; altsaa

5 er $R$ for $p = 10n + 1$ og $10n + 9$, $I$ for $p = 10n + 3$ og $10n + 7$

og følgelig

$-5$ er $R$ for $p = 20n + 1$, $20n + 3$, $20n + 7$, $20n + 9$, $I$ for $p = 20n + 11$, 13, 17, 19.

I Almindelighed faa vi for $p = 4n + 1$, $\alpha = 1, 2, 3 \ldots p - 1$

$$\left(\frac{p}{np+\alpha}\right) = \left(\frac{\alpha}{p}\right) = +1 \text{ eller } -1,$$

eftersom $\alpha$ er $R$ eller $I$ for $p$; da imidlertid eftersom $n$ er lige eller ulige, $\alpha$ maa være ulige eller lige, sættes bedre $2n$ for $n$; $\alpha$ er da ulige, men gaar til $2p$. Er $p = 4n + 3$, tager vi for det søgte Primtal Formen $4np + \alpha$ for lettere at se, naar Symbolet skal skifte Tegn ved Brøkens Omvending.

68. Vi kunne ad denne Vej udlede Formen af Primfaktorerne i Tal af Formen $x^2 + ay^2$; ($x$ pr. med $ay$). Sætte vi nemlig, idet $k$ er en Primfaktor i Tallet

$$yz \equiv x \pmod{k}$$

bestemmes derved en Værdi af $z$, og vi faa

$$x^2 + ay^2 \equiv y^2z^2 + ay^2 = y^2(z^2 + a) \pmod{k}$$

der, da $k$ ikke gaar op i $y$, viser, at:

En Primfaktor, der findes i et Tal $x^2 + ay^2$, hvor $x$ pr. med $y$, findes ogsaa i et Tal af Formen $x^2 + a$.

Vi faa saaledes, idet vi stadig forudsætte $x$ pr. med $y$ og med $a$ og undtage Faktoren 2:

Alle Primfaktorer i $x^2 + y^2$ ere af Formen $4n + 1$.

Alle Primfaktorer i $x^2 - 2y^2$ ($x$ ulige) ere af Formerne $8n \pm 1$.

Alle Primfaktorer i $x^2 + 2y^2$ ($x$ ulige) ere af Formerne $8n + 1$ og $8n + 3$.

Alle Primfaktorer i $x^2 - 3y^2$ ($x$ ikke delelig med 3) ere af Formerne $12n \pm 1$.

Alle Primfaktorer i $x^2 + 3y^2$ ($x$ ikke delelig med 3) ere af Formen $6n + 1$.

Alle Primfaktorer i $x^2 - 5y^2$ ($x$ ikke delelig med 5) ere af Formerne $10n \pm 1$, og saaledes videre.

*Fermat* angav uden Bevis de Tal, for hvilke — 1 og $\pm 2$ ere Rester*). Bevis søgtes uden Held af Euler, men fandtes af Lagrange, der ogsaa undersøgte Tallene $\pm 3$, $\pm 5$, $\pm 7$**). Hans Fremgangsmaade var meget besværlig.

*) Opera Math. Pg. 168.
**) Nouv. Mém. de l'Ac. de Berlin 1775.



69. Udtryk af Formen $x^2 + ay^2$ have den mærkelige Egenskab, at Produktet af to saadanne (med samme Værdi af $a$) kan skrives under samme Form; man har nemlig indentisk

$$(9) \qquad (a + b\sqrt{-c})\,(m \mp n\sqrt{-c}) = x + y\sqrt{-c},$$

hvor

$$(10) \qquad x = am \pm cbn\,;\; y = an \mp lm$$

og ligeledes

$$(11) \qquad (a - b\sqrt{-c})\,(m \pm n\sqrt{-c}) = x - y\sqrt{-c}.$$

Ved Multiplikation faa vi nu

$$(12) \qquad (a^2 + cb^2)\,(m^2 + cn^2) = x^2 + cy^2,$$

hvor vi forudsætte, at $a$, $b$, $m$ og $n$ og derfor ogsaa $x$ og $y$ ere hele Tal. Vi kunne nu bevise følgende Sætning:

Dersom i et Tal $x^2 + cy^2$ en Primfaktor har samme Form, maa den anden Faktor ogsaa have den.

Man faar nemlig af Ligningerne (10)

$$(13) \qquad a = \frac{mx \pm cny}{m^2 + cn^2}\,;\; = b\,\frac{nx \mp my}{m^2 + cn^2},$$

hvor vi faa de dobbelte Fortegn ved at tage $y$ baade positiv og negativ, medens Fortegnene for $a$ og $b$, der skulle kvadreres, ere uden Betydning. Nu gaar $m^2 + cn^2$ op i

$$m^2(x^2 + cy^2) - cy^2(m^2 + cn^2) = (mx + cny)\,(mx - cny)$$

og i

$$n^2(x^2 + cy^2) - y^2(m^2 + cn^2) = (nx + my)\,(nx - my).$$

Hvis nu $m^2 + cn^2$ er et Primtal, maa det gaa op i en af Faktorerne i hvert af disse Produkter, saa at een Værdi for $a$ og een Værdi for $b$ blive hele Tal, og at

disse ere de sammenhørende Værdier følger af Identiteten

$$(mx \pm cny)^2 + c\,(nx \mp my)^2 = (m^2 + cn^2)\,(x^2 + cy^2),$$

der viser, at naar $m^2 + cn^2$ gaar op i $nx \mp my$, gaar det ogsaa op i $mx \mp cny$.

70. Da der til et Par givne Værdier af $x$ og $y$ saaledes svarer et Par hele Værdier af $a$ og $b$, maa man ved at benytte (9) eller (10) faa alle Værdier af $x$ og $y$, naar man har alle Værdier af $a$ og $b$, altsaa:

Naar man multiplicerer et Primtal $m^2 + cn^2$ med et vilkaarligt Tal $a^2 + cb^2$, vil man ved Anvendelse af (9) eller (10) faa Produktet skrevet paa alle mulige Maader, naar man har $a^2 + cb^2$ paa alle Maader.

Heraf følger atter:

Alle Løsninger af $x^2 + cy^2 = p$, hvor $p$ er et Primtal, faas af een Løsning og af alle Løsninger af $x^2 + cy^2 = 1$.

For $c$ positiv har den sidste Ligning kun Løsningen $x = 1$, $y = 0$ (idet vi ikke gøre Forskel paa $+1$ og $-1$, der give samme Værdi for $x^2$), altsaa

Et Primtal kan kun paa een Maade skrives paa Formen $x^2 + cy^2$, naar $c$ er positiv.

Dette forudsætter naturligvis, at $-c$ er kvadratisk Rest for $p$; i modsat Fald har Ligningen ingen Løsninger. Er $c$ positiv, faar saaledes Ligningen

$$x^2 + cy^2 = A \tag{14}$$

ingen eller et endeligt Antal Løsninger, medens Ligningen



$$x^2 - cy^2 = A \tag{15}$$

faar ingen eller uendelig mange Løsninger; da dette hidrører fra, at vi faa uendelig mange Løsninger for $A = 1$, ville vi nærmere undersøge dette Tilfælde, idet vi forudsætte, at $c$ ikke er et Kvadrattal.

71. Vi ville altsaa nærmere undersøge Ligningen

$$x^2 - cy^2 = 1\,^{*)} \quad (c \text{ positiv}). \tag{16}$$

Da i denne Ligning $x$ og $y$ samtidig maa vokse eller aftage, kunne vi tale om større og mindre Løsninger, og navnlig ville vi ved den mindste Løsning forstaa den, hvor $x$ og $y$ ere hele Tal med de mindst mulige numeriske Værdier. Ere disse $\alpha$ og $\beta$ ($\beta$ ikke Nul), kunne vi da vise, at alle Løsninger bestemmes ved Ligningen

$$x + y\sqrt{c} = (\alpha + \beta\sqrt{c})^n, \tag{17}$$

hvor $n$ gennemløber alle positive hele Værdier.

Gaa vi ud fra $\alpha + \beta\sqrt{c}$, faa vi for hver Gang vi multiplicere med $\alpha + \beta\sqrt{c}$ en højere Løsning, medens vi gaa tilbage i Rækken af Løsninger, naar vi multiplicere med $\alpha - \beta\sqrt{c}$, da denne Multiplikation er identisk med Division med $\alpha + \beta\sqrt{c}$.

Gaa vi nu ud fra en vilkaarlig Løsning, og danne vi af denne mindre Løsninger ved successive Divisioner med $\alpha + \beta\sqrt{c}$, maa vi omsider komme til $\alpha + \beta\sqrt{c}$, da der i modsat Fald maatte gives mindre Løsninger. Den Løsning, vi gik ud fra, maa derfor høre til den ovenfor bestemte Række af Løsninger. Det gælder saaledes ved Ligningens Løsning kun om at finde den laveste

*) Se Indledningen Pg. 9.

Løsning; vi komme senere tilbage hertil; vi ville blot bemærke, at man ikke kan vente at finde den laveste Løsning ved Forsøg, da den, selv ved smaa Værdier af $c$, kan have meget store Værdier af $\alpha$ og $\beta$.

For Eks. for $c = 661$, faar den laveste Værdi af $x$ 38 Cifre.

Er $c$ et Kvadrattal, er der ingen andre Løsninger end $x = 1$; $y = 0$.

72. Vi ville nu særlig undersøge Ligningen

$$x^2 + y^2 = a, \tag{18}$$

hvor vi, naar vi tale om Antallet af Løsninger, ikke gøre Forskel paa saadanne, der kun ere forskellige ved Fortegnene ved $x$ og $y$ eller ved, at disse ere ombyttede. Vi vide, at hvis $x$ og $y$ ere indbyrdes pr., kan $a$ kun indeholde ulige Primfaktorer af Formen $4n + 1$; hvis der derfor i $a$ findes en Primfaklor af Formen $4n + 3$, maa den være fælles Faktor for $x$ og $y$ og findes i $a$ med lige Eksponent; altsaa:

Indeholder $a$ en Primfaktor $4n + 3$ med ulige Eksponent er Opgaven umulig.

Antag nu $a = 2^q$; for $q = 1$ have vi kun Løsningen $x = y = 1$ og faa saa med en let forstaaelig Betegnelse

$$(1 + \sqrt{-1})(1 \pm \sqrt{-1})(1 \pm \sqrt{-1}) \ldots (q \text{ Fakt.}) = (2^q)$$

Nu er imidlertid

$$1 - \sqrt{-1} = -\sqrt{-1}\,(1 + \sqrt{-1}),$$

saa at Ligningen kan skrives

$$(2^q) = (1 + \sqrt{-1})^q \tag{19}$$



idet en Faktor $(\sqrt{-1})^a$ kun kan gøre, at $x$ og $y$ ombyttes. Altsaa:

Naar $a$ er en Potens af 2, har Ligningen kun een Løsning.

Er $a = p^q$, hvor $p = 4n + 1$ og er

$$\alpha + \beta\sqrt{-1} = (p),$$

faar man

$$(p^q) = (\alpha + \beta\sqrt{-1})^\mu\,(\alpha - \beta\sqrt{-1})^\nu\quad(\mu + \nu = q) \tag{20}$$

saa at Udtrykket faar $q + 1$ Værdier; af disse ere imidlertid for $q$ ulige to og to kun forskellige ved Fortegnet for $\sqrt{-1}$, medens for $q$ lige den som svarer til $\mu = \nu = \frac{1}{2}q$ ikke forandres ved Ombytningen, vi faa altsaa henholdsvis $\frac{1}{2}(q + 1)$ eller $\frac{1}{2}(q + 2)$ Løsninger.

Indeholder $a$ andre analoge Primtalspotenser, maa vi multiplicere (20) med de analoge Udtryk. I Resultatet ville da to og to Udtryk kun være forskellige ved Fortegnet for $\sqrt{-1}$, med mindre alle Eksponenterne ere lige, da et af Udtrykkene ikke forandres ved Ombytningen. Altsaa:

Er $$a = 2^q\,p_1^{q_1}\,p_2^{q_1}\ldots,$$

hvor Primfaktorerne $p$ ere af Formen $4n + 1$, er Løsningernes Antal

$$\frac{1}{2}(p_1 + 1)(q_2 + 1)\ldots \tag{21}$$

hvortil maa adderes $\frac{1}{2}$, hvis $q_1, q_2 \ldots$ alle ere lige.

Dersom vi gøre Forskel paa de Løsninger, hvor blot $x$ og $y$ ere ombyttede, bliver Antallet

$$(q_1 + 1)(q_2 + 1)(q_3 + 1)\ldots,$$

hvortil der skal adderes 1, dersom alle $q$ ere lige, altsaa hvis Tallet er et Kvadrat eller det dobbelte af et Kvadrat. I det første Tilfælde regne vi herved $0 + a^2$ og $a^2 + 0$ for to Løsninger, i det sidste regne vi $a^2 + a^2$ for to Løsninger. Dersom vi derfor fastsætte, at vi kun regne den sidste for een Løsning, og at den ene af de ubekendte ikke maa være Nul, er Løsningernes Antal altid

$$(q_1 + 1)(q_2 + 1)(q_3 + 1)\ldots \tag{22}$$

Dette Tal angiver netop Antallet af Divisorer i Tallet, naar vi af dette bortfjærne alle Primfaktorer 2 og $4n+3$ eller i Følge 6 Antallet af Divisorer af Formen $4n+1$, minus Antallet af Divisorer af Formen $4n+3$.

Indeholder $a$ Primfaktorer $4n+3$ med lige Eksponenter, forandres Løsningernes Antal ikke.

73. Enhver Divisor i en Sum af to indbyrdes primiske Kvadrattal er selv en Sum af to Kvadrattal.

Vi sætte

$$a^2 + b^2 = pq,$$

hvor $p$ er den mindste Primfaktor og antage, at Sætningen er bevist for lavere Værdier af Kvadratsummen. $a$ og $b$ kunne ikke begge være mindre end $\frac{1}{2}p$ og maa derfor ved Division med $p$ kunne give Rester (positive eller negative), af hvilke i det mindste den ene er mindre end Dividenden; vi komme derved, idet vi kalde Resterne $\alpha$ og $\beta$ til en ny Ligning af Formen

$$\alpha^2 + \beta^2 = mp.$$

Hverken $\alpha$ eller $\beta$ kan være Nul, og have de en fælles Faktor, maa denne findes i $m$ og tænkes bort-



divideret. Da nu $\alpha^2 + \beta^2 < a^2 + b^2$, gælder Sætningen i Følge vor Forudsætning for den ny Ligning og $p$ er derfor en Sum af to Kvadrater. Det samme gælder da i Følge 69 om $q$, og da $q < a^2 + b^2$, om $q$'s Divisorer, altsaa om $a^2 + b^2$.

74. Ethvert Primtal af Formen $4n+1$ kan skrives som en Sum af to Kvadrattal.

Ifølge Wilsons Sætning gaar Primtatlet op i

$$(1 \cdot 2 \cdot 3 \ldots 4n + 1)$$

eller, da de sidste $2n$ Tal ere kongruente med de første $2n$ med modsatte Fortegn i

$$(1 \cdot 2 \cdot 3 \ldots 2n)^2 + 1$$

Da Primtallet saaledes gaar op i en Sum af to Kvadrater, er det i Følge den forrige Sætning selv en saadan Sum.

*Eks. 1.*

$$x^2 + y^2 = 5 \cdot 13^2$$

$$2 + \sqrt{-1} + (5);\ (3 + 2\sqrt{-1}) = (13)$$

$$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 + 2\sqrt{-1})^2 \quad x = 2;\ y = 29$$

$$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 - 2\sqrt{-1})(3 + 2\sqrt{-1})$$

$$x = 26;\ y = 13$$

$$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 - 2\sqrt{-1})^2 \quad x = 22;\ y = 19$$

*Eks. 2.* $\quad x^2 + y^2 = 5 \cdot 13^2 \cdot 19^2$

Løsningerne faas ved at multiplicere de foregaaende med 19.

75. Om Ligningen

$$x^2 + 2y^2 = a \tag{23}$$

vide vi, at hvis $x$ og $y$ ere indbyrdes primiske, maa alle ulige Primfaktorer i $a$ være af en af Formerne $8n + 1$ eller $8n + 3$. Hvis derfor $a$ har Primfaktorer af Formerne $8n + 5$ eller $8n + 7$, maa disse forekomme med lige Eksponenter og blive fælles Faktorer for $x$ og $y$. Altsaa

Indeholder $a$ Primfaktorer $8n + 5$ eller $8n + 7$ med ulige Eksponent er Opgaven umulig.

For $a = 2$ have vi

$$0 = \sqrt{-2} = (2)$$

og derfor

$$(\pm\sqrt{-2})^q = (2^q)$$

som viser, at:

Naar $a$ er en Potens af 2, har Opgaven kun een Løsning.

Er $a = p^q$ og have vi

$$\alpha + \beta\sqrt{-2} = (p)$$

hvad der nødvendigvis kræver, at $p$ er af en af Formerne $8n + 1$, $8n + 3$, faa vi

$$(p^q) = (\alpha + \beta\sqrt{-2})^\mu (\alpha - \beta\sqrt{-2})^\nu, \ (\mu + \nu = q)$$

der giver $q + 1$ Værdier; har $a$ flere analoge Faktorer, maa vi multiplicere med de analoge Udtryk. Ganske som for $c = -1$ faa vi da Antallet

$$\frac{1}{2}(q_1 + 1)(q_2 + 1)\ldots$$

hvor vi maa addere $\frac{1}{2}$, hvis alle $q$ ere lige Tal.



Saaledes for $a = 11 . 17$ faa vi

$$(11) = 3 \pm \sqrt{-2}\,; (17) = 3 \pm \sqrt{-2}$$

$$(187) = (3 + \sqrt{-2})(3 + 2\sqrt{-2}) + 5 + 9\sqrt{-2}\,; (3 + \sqrt{-2})$$
$$(3 - 2\sqrt{-2} = 13 - 3\sqrt{-2},$$

saa at vi faa $\frac{1}{2} . 2 . 2 = 2$ Løsninger, nemlig

$$187 + 5^2 + 2 . 9^2 = 13^2 + 2 . 3^2$$

For $a = 17^2$ faa vi paa samme Maade

$$(289) = (3 \pm 2\sqrt{-2})^2 = 1 \pm 12\sqrt{-2}\,; (3 + 2\sqrt{-2}$$
$$(3 - 2\sqrt{-2}) = 17$$

altsaa 2 Løsninger, hvis $y$ tør være Nul, nemlig

$$289 = 1 + 2 . 12^2 = 17^2$$

Primfaktorer $8n + 5$ og $8n + 7$ forandre ikke Løsningernes Antal, hvis deres Eksponenter ere lige, men gøre Opgaven umulig, hvis nogen af dem har ulige Eksponent.

76. Enhver Faktor i $x^2 + 2y^2$, hvor $x$ er pr. med $2y$, har samme Form.

Beviset føres ganske som for en Sum af to Kvadrattal.

Ethvert Primtal $8n + 1$ eller $8n + 3$ kan skrives (og det kun paa een Maade), paa Formen $x^2 + 2y^2$.

Ethvert saadant Primtal $p$ maa nemlig findes som Divisor i visse Tal $x^2 + 2y^2$, da Kongruensen

$$x^2 + 2 \equiv 0 \ (\text{mod. } p)$$

altid har Løsninger.

77. Vi ville endnu undersøge Ligningen

$$x^2 + 3y^2 = a. \tag{24}$$

Hvis $a$ er delelig med 3, kan denne Faktor bortdivideres, uden at Ligningens Form forandres. Er $a$ lige, maa $x$ og $y$ begge være lige eller begge ulige; i det første Tilfælde kan 4 bortdivideres, uden at Ligningens Form forandres. I det andet Tilfælde kan 4 ogsaa bortdivideres, idet $(2n+1)^2 + 3(2n+1)^2$ er delelig med 4. Idet vi sætte $4 = 1^2 + 3 \cdot 1^2$ kunne vi benytte (13) og faa derved

$$\frac{(2n+1)^2 + 3(m+1)^2}{1^2 + 3 \cdot 1^2} = \alpha^2 + 3\beta^2$$

hvor

$$\beta = \frac{2n + 1 \pm (2m+1)}{4}$$

der maa give en hel Værdi, da af to ulige Tal enten Summen eller Differensen er delelig med 4. Til den hele Værdi af $\beta$ maa svare en hel Værdi af $\alpha$, og 4 kan saaledes bortdivideres uden at Ligningens Form forandres. Vi se ogsaa, at hvis $a$ er lige, men ikke delelig med 4, er Opgaven umulig.

Vi have vist, at hvis $x$ og $y$ ere indbyrdes primiske, maa alle Primfaktorer i $a$ være af Formen $6n+1$; hvis derfor $a$ har Primfaktorer af Formen $6n+1$, maa disse findes i $x$ og $y$ og findes i $a$ med lige Eksponenter.

Idet vi nu gaa frem som i de foregaaende Tilfælde, faa vi

Naar $a$ er et ulige Tal, hvis Primfaktorer $6n-1$ har lige Eksponenter, medens Primfaktorerne $6n+1$ have Eksponenterne $q_1$, $q_2 \ldots$, har Ligningen $x^2 + y^2 = a$.



$$\frac{1}{2}(q_1 + 1)(q_2 + 1)\ldots \tag{25}$$

Løsninger:

Tilføje vi Faktoren 4, bliver Løsningernes Antal 3 Gange saa stort, da vi ikke alene faa saadanne ved at multiplicere med $1 \pm \sqrt{-3}$, men ogsaa ved at multiplicere med 2. Saaledes er $7 = 2^2 + 3 \cdot 1^1$, men

$$28 = 1^2 + 3 \cdot 3^2 = 4^2 + 3 \cdot 2^2 = 5^2 + 3 \cdot 1^2$$

Yderligere Tilføjelser af Faktoren 4 forøger ikke Løsningernes Antal, idet man blot skal multiplicere de tidligere Løsninger med Potenser af 4. Grunden hertil ligger i at

$$(1 + \sqrt{-3})^2 = -2(1 - \sqrt{-3})\,;\, (1 + \sqrt{-3})^3 = -8.$$

Saaledes faar man den fuldstændige Løsning

$$112 = 2^2 + 3 \cdot 6^2 = 8^2 + 3 \cdot 4^2 = 10^2 + 3 \cdot 2^2.$$

Sætte vi

$$a^2 + 3b^2 = pq,$$

hvor $p$ er den mindste Primfaktor kunne vi ikke have baade $a$ og $b$ lig eller mindre end $\frac{1}{2}(p-1)$, da deraf vilde følge

$$a^2 + 3b^2 \overline{\gtrless} (p-1)^2,$$

som strider mod, at $p$ er den mindste Primfaktor. Vi kunne da gaa frem som tidligere og faa, idet vi betragte 4 som et Primtal:

Alle Divisorer i et Tal $x^2 + 3y^2$, hvor $x$ og $3y$ ere indbyrdes pr., kunne skrives paa samme Form, og

Ethvert Primtal $6n+1$ kan skrives (og det kun paa een Maade) paa Formen $x^2 + 3y^2$.

78. De her behandlede Former ere specielle Tilfælde af de almindelige kvadratiske Former, men have en særlig historisk Interesse, idet de fleste af de nævnte Sætninger ere fremsatte af Fermat og beviste af Brownker, Euler, Lagrange, Legendre o. fl., dog ad andre Veje end de her benyttede. Vi ville hertil knytte et Par Sætninger, som ogsaa falde ind under den almindelige Teori, men som vi med de Midler, vi nu have til Raadighed, kunne give simple Beviser for.

Dersom vi i Ligningen

$$x^2 + y^2 = a$$

for $x$ og $y$ indsætte alle hele positive Tal, for $y$ tillige Nul, faa vi for $a$ alle de Værdier, for hvilke Ligningen har Løsninger, og hver Værdi $a$ faas netop saa mange Gange, som der er Løsninger, idet vi regne $m^2 + n^2$ og $n^2 + m^2$ for to Løsninger, naar $m$ og $n$ ere forskellige, og ingen af dem er Nul. Vi ville nu vise, at alle Værdierne af $a$, enhver af dem det fundne Antal Gange, kunne faas frem paa en hel anden Maade.

Lad os betragte to Rækker af Tal

$$1, 2, 3, 4 \ldots$$
$$1, -3, +5, -7, +9, \ldots$$

Den første indeholder alle positive, hele Tal, den anden alle ulige Tal, dog saaledes, at alle de, der have Formen $4n + 3$, faa Fortegnet —. Vi multiplicere nu ethvert af Tallene i den ene Række med ethvert af Tallene i den anden Række, og ville bevise, at vi derved netop faa alle Tallene $a$, ethvert af dem det rigtige Antal Gange (idet vi regne, at $+a$ og $-a$ hæve hinanden). Dette Antal Gange er ifølge 72

$$(q_1 + 1)\,(q_2 + 1) \ldots,$$



naar der i $a$ forekommer Primfaktorer $4n + 1$ med Eksponenterne $q_1$, $q_2 \ldots$ medens andre Primfaktorer ikke have Indflydelse paa Antallet.

Lad nu $a$ være et ulige Tal, der har mindst en Primfaktor $4n + 3$ med ulige Eksponent. Ifølge 72 har $a$ da lige mange Divisorer $4n + 1$ og $4n + 3$. Lad os nu i den første Række opsøge alle Divisorerne, altsaa lige mange af hver af de to Former. Er $a$ af Formen $4n + 3$, maa det første Sæt Divisorer multipliceres med negative Tal af den anden Række, det andet med positive, omvendt, hvis $a$ er af Formen $4n + 1$. I begge Tilfælde faar man altsaa, at $a$ forekommer Nul Gange, stemmende med, at Ligningen for saadanne $a$ er uden Løsninger.

Har $a$ ingen Primfaktor $4n + 3$, bliver alle Produkterne positive og vi faa derfor $a$ saa mange Gange som der er Divisorer, stemmende med Antallet af Ligningens Løsninger i dette Tilfælde.

Indeholder $a$ en Primfaktor $4n + 3$ med lige Eksponent, kan den bortkastes; have vi saaledes Faktoren $7^4$, have vi i øverste Række, idet $m$ er en Faktor

$$m \,.\, 7 \quad m \,.\, 7^2 \quad m \,.\, 7^3 \quad m \,.\, 7^4,$$

hvortil svare i nederste Række Tal af Formen

$$n \,.\, 7^3, \quad n \,.\, 7^2 \quad n \,.\, 7 \quad n \,.\, 1,$$

der afvekslende ere positive og negative. Vi kunne derfor udelade i den første Række alle Divisorer, der indeholde Faktoren $4n + 3$ og Resultatet er saaledes det samme, som om denne Faktor manglede, stemmende med det vi vide om Ligningens Løsninger i dette Tilfælde.

Indeholder endelig $a$ Faktoren $2^r$ kunne vi af den første Række kun tage Tal, der ere delelige med $2^r$. Det søgte Antal Gange er derfor det samme, som om denne

Faktor manglede. Hermed er Sætningen fuldstændig bevist.

Idet vi multiplicere hvert Tal af første Række med hvert Tal af anden Række, danne vi de samme Produkter, som vi multiplicerede Summen af Tallene i første Række med Summen af Tallene i anden Række; disse Summer ere imidlertid meningsløse, da de danne divergente Rækker. Nu er imidlertid Samlingen af Tallene $a$ identisk med Samlingen af Produkter, vi danne, og denne Identitet maa vedblive at finde Sted, naar vi begge Steder for ethvert Tal sætte en bestemt Funktion af Tallet, og det gælder da om, at vælge denne Funktion saaledes, at Summerne af Tallene i begge vore Samlinger give konvergente Rækker. Dette bliver Tilfældet, naar vi for ethvert af Tallene $n$ sætter $n^{-s}$, hvor $s$ er et vilkaarligt reelt eller komplekst Tal, hvis reelle Del er positiv og større end 1.

Vi faa saaledes den mærkelige Ligning

$$(26)\qquad \ldots \Sigma \frac{1}{(x^2+y^2)^s} = \left(1+\frac{1}{2^s}+\frac{1}{3^s}+\ldots\right)$$
$$\left(1-\frac{1}{3^s}+\frac{1}{5^s}+-\frac{1}{7^s}+\ldots\right),$$

hvor ved Summationen $x$ skal antage alle Værdierne 1, 2, 3 . . ., $y$ de samme Værdier og tillige Værdien Nul.

Ved at gaa frem paa samme Maade faar man

$$(27)\qquad \Sigma \frac{1}{(x^2+2y^2)^s} = \left(1+\frac{1}{2^s}+\frac{1}{3^s}\ldots\right)\left(1+\frac{1}{3^s}-\frac{1}{5^s}-\frac{1}{7^s}+\frac{1}{9^s}+\ldots\right),$$

hvor $x$ og $y$ ere alle negative Tal, $x$ tillige Nul og alle positive Tal, $y$ tillige Nul. I den anden Parentes ere de Led negative, hvor Tallet i Nævneren er af Formen $8n+5$ eller $8n+7$.



## Tchebychefs Formel for Antallet af Primtal under en given Grænse.

1. Skønt Faktorerne i Tæller og Nævner af de for de mindste fælles Multiplum angivne Udtryk (21) og (24) ere stærkt af- tagende, kan man ikke danne Tilnærmelsesformler ved simpelt hen at afbryde Brøkerne, da de saaledes dannede Brøker ikke afvekslende ere for store og for smaa. Tilnærmelsesværdier kunne derimod dannes, idet man danner lignende Udtryk, der i Begyndelsen stemmer med Formlerne, og hvor de følgende Faktorer vælges saaledes, at Brøken kommer til at indeholde de Primfaktorer, man ønsker; det bliver her, som det vil ses af det følgende, nødvendigt, at Brøkerne i Tælleren og Nævneren have samme Sum. Saaledes faar man en lavere Grænse ved at benytte den af Tchebychef angivne Brøk.

$$\varphi(n) = \frac{[n]\left[\frac{n}{30}\right]}{\left[\frac{n}{2}\right]\left[\frac{n}{3}\right]\left[\frac{n}{5}\right]}$$

hvor $1+\frac{1}{30}=\frac{1}{2}+\frac{1}{3}+\frac{1}{5}$. Er $n=\alpha p+\beta$, hvor $p$ er et Primtal og $\beta<p$, vil $p$ forekomme med Exponenten

$$a-\left(\frac{\alpha}{2}\right)-\left(\frac{\alpha}{3}\right)-\left(\frac{\alpha}{5}\right)+\left(\frac{\alpha}{30}\right)$$

plus analoge Udtryk, dersom $n>p^2$ o. s. v. Man finder heraf for $\alpha = 1, 2, \ldots . 30$

111110111010110010100010000010,

hvor man lettest danner hvert Tal af det foregaaende, idet man undersøger, hvilke af Tallene $\alpha\left(\frac{\alpha}{2}\right)\ldots$, der

blive hele. Man ser heraf, at Brøken indeholder alle Primtallene, hvert 1 Gang, undtagen for $\alpha = 6, 10, 12$ o. s. v. For $\alpha > 30$ kommer de samme Værdier periodisk igen. For $p < \sqrt{n}$ findes Eksponenten, i Følge (1), ved at addere flere Tal i Rækken ovenfor, men da disse alle ere 1 og 0, medens de for mindste fælles Multiplum alle ere 1, kan Eksponenten ikke overstige den, med hvilken Primtallet forekommer i mindste fælles Multiplum. Brøken gaar derfor op i mindste fælles Multiplum og er saaledes en lavere Grænse for dette. Man ser Nødvendigheden af, at de to ovenfor omtalte Summer ere lige store, idet Periodiciteten betinges af, at man i Rækken faar Nul for $\alpha = 30$. Anvende vi nu paa Rækken den bekendte Formel

$$l\,.\,[n] = l\,.\,\sqrt{2n\pi} + nl\,.\,n - n$$

hvor Fejlen er mindre end $\frac{1}{12n}$, og derfor, naar $n$ ikke er for lille, kan lades ude af Betragtning, faa vi, idet $M_n$ er mindste fælles Multiplum, og $n$ tænkes delelig med 30,

$$l\,.\,M_n > n\,l\,.\,\frac{2^{\frac{1}{2}}\,.\,3^{\frac{1}{3}}\,.\,5^{\frac{1}{5}}}{30^{\frac{1}{30}}} - l\,.\,\sqrt{2n\pi}$$

Er $P$ Antallet af Primtal indtil $n$ (1 ikke medregnet), har man $n^P > M_n$, idet ingen af de i $M_n$ forekommende Potenser af et Primtal kan overstige $n$. Man faar altsaa

$$n^P > \left(\frac{2^{\frac{1}{2}}\,.\,3^{\frac{1}{3}}\,.\,5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right)^n : \sqrt{2n\pi}$$

eller

$$P > \frac{0{,}4001\,.\,n}{\log.\,n}$$



idet Divisoren $\sqrt{2n\pi}$ bliver af forsvindende Betydning, da det derfra hidrørende Led er en ægte Brøk.

Den saaledes fundne lavere Grænse for Antallet af Primtal indtil $n$ er lidt bedre end den af Tchebychef angivne. Til Bedømmelse af Afvigelsen tjener, at Formlen

$$P = \frac{0{,}5\,.\,n}{\log.\,n}$$

passer meget godt til omtrent $n = 3000$; den giver f. Eks. for $n = 100, 1000, 2000, 3000$

$$P = 25,\ 168,\ 222,\ 303,\ 430.$$

For større Tal giver den Antallet for stort; for 100 Mill. maatte man f. Eks. for $0{,}5$ sætte $0{,}461$.

2. For at finde en højere Grænse for $M_n$ betragte vi Produktet

$$\varphi(n)\,.\,\varphi\left(\frac{n}{6}\right)\,.\,\varphi\left(\frac{n}{6^2}\right)\ldots$$

Den Række Tal, der angiver Eksponenterne for $p$, har sit første 0 for $\alpha = 6$; den der svarer til $\varphi\left(\frac{n}{6}\right)$, faar 1 for $\alpha = 6$ og sit første Nul for $\alpha = 36$; adderes de to Rækker, faar den nye Række sit første Nul for $\alpha = 36$, medens de foregaaende Tal blive 1 og 2; adderes Rækken for $\varphi\left(\frac{n}{6^2}\right)$ hertil, faar den nye Række sit første Nul for $\alpha = 216$ o. s. v. Produktet indeholder derfor alle Primfaktorer i samme eller højere Potens end den, i hvilken de findes i $M_n$, saa at man har

$$M_n < \varphi(n)\,\varphi\left(\frac{n}{6}\right)\varphi\left(\frac{n}{6^2}\right)\ldots$$

Enhver af disse Faktorer er mindre end den sjette Rod af den forrige; thi, idet $k$ er den tidligere beregnede Konstant, er

$$\varphi(n) = \frac{k}{\sqrt{2n\pi}}\ ;\ \varphi\left(\frac{n}{6}\right) = \frac{k^{\frac{n}{6}}}{\sqrt{\frac{n}{6}\pi}} < \frac{k^{\frac{n}{6}}}{\sqrt[12]{2n\pi}}$$

Altsaa er $M_n < \varphi(n)^{1+\frac{1}{6}+\frac{1}{6^2}+\cdots} = \varphi(n)^{\frac{6}{5}}$,

saa at $$\log. M_n < 0{,}4801\, n,$$

altsaa, naar vi for Simpelheds Skyld kan benytte 2 Decimaler

$$0{,}40\, n < \log. M_n < 0{,}48.$$

---